ISSN: 3061-8991

Vol. 1 / 2025

Actas de Ciberseguridad para la Industria 5.0

Ciencia y Tecnología
Secretaría de Ciencia, Humanidades, Tecnología e Innovación
INAOE

Actas de Ciberseguridad para la Industria 5.0

ISSN: 3061-8991

Actas de Ciberseguridad para la Industria 5.0 Vol. 1 (2025) es una publicación anual editada por el Instituto Nacional de Astrofísica Óptica y Electrónica, Calle Luis Enrique Erro, 1, Santa María Tonantzintla, San Andrés Cholula, C.P. 72840, Puebla, Pue., Tel. 2222663100, ext. 8303, página electrónica de la revista: https://actasciberseguridad.inaoep.mx/, Correo electrónico: actas.rci@inaoep.mx.
Editor responsable: Dr. Miguel Morales Sandoval. Reserva de Derechos al Uso Exclusivo No. 04-2025-070114531400-102, ISSN: 3061-8991, ambos otorgados por el Instituto Nacional del Derecho de Autor.
Responsable de la última actualización de este número, Lic. Liliana Perea Centeno, Instituto Nacional de Astrofísica Óptica y Electrónica, Calle Luis Enrique Erro, 1, Santa María Tonantzintla, San Andrés Cholula, C.P. 72840, Puebla, Pue., fecha de última modificación: Julio de 2025. Tamaño del archivo: 38MB.

Contenido

Editorial

La ciberseguridad ha cobrado un papel relevante para proteger los activos digitales de la industria y de las organizaciones. Con el avance en las técnicas de ataque, motivadas principalmente por el uso de inteligencia artificial generativa, es necesario desarrollar soluciones de ciberseguridad novedosas, en áreas como el Internet de las Cosas, el Cómputo en la Nube, la Inteligencia Artificial y la Ciencia de Datos, entre los más relevantes. Desde la investigación y el desarrollo tecnológico, la difusión de conocimiento contribuye a la prevención, detección y reacción a ataques que pueden poner en riesgo la seguridad de activos digitales.

En este primer número de la revista *Actas de Ciberseguridad para la Industria 5.0* se presentan veintiún artículos, todos presentados en la serie de Reuniones de Ciberseguridad: la Primera y Segunda *Reunión de Ciberseguridad para la Industria 4.0 –RCI4.0*, realizada en 2018 y 2019, respectivamente; así como en la Tercera *Reunión de Ciberseguridad para la Industria 5.0 –RCI5.0* realizada en 2024. Estos foros han permitido la convergencia de practicantes, investigadores y estudiantes en el área de Ciberseguridad, en donde se presentaron y discutieron problemáticas actuales del área, los avances más recientes en investigación y aplicaciones futuras en la industria.

Los primeros seis artñiculos de este número están orientados a las aplicaciones en ciberseguridad. Justiniano et al., proponen una configuración que permita cumplir con los estándares de seguridad requeridos actualmente en una VPN. Carrión Martínez et al., describen un sistema embebido para el control de acceso mediante el uso de tecnología RFID, en conjunto con un módulo de reconocimiento de expresiones faciales. Grajales-Flores et al., describen la implementación y aspectos de seguridad de un esquema que realiza la alineación automática de un arreglo de cámaras. Reyes-Aldeco et al., presenta un sistema basado en la red neuronal YOLO V3 con el objetivo de detectar armas en un conjunto de imagenes de asaltos, prácticas de tiro y documentales. Reyes-Macedo et al., muestran un panorama general sobre la normatividad internacional de la privacidad en el contexto de la cuarta revolucion industrial. Carrión Martínez et al., proponen un dispositivo electronico utilizando un sistema embebido basado en microcontroladores que incorpora un esquema de seguridad para evitar que los datos sean alterados por algun elemento externo antes, durante o después de que ocurra un accidente automovilístico. Finalmente, Castillo Rosete et al., describen la implementación de un sistema para señalización vía SSH para comunicar por medio de Ethernet y/o WiFi el software App Inventor y el Hardware Arduino Yun, para monitoreo y control remoto del encendido y apagado de una carga a 110 volts.

Los siguientes cuatro artículos están orientados a la tecnología Blockchain. Reyes-Macedo et al., hacen una revisión de los estudios que han evaluado propuestas para anonimato y privacidad, y de aquellos que han contribuido a robustecer dichos servicios. Ayala Zamorano et al., abordan el concepto de tokenización, enfatizando los algoritmos existentes para generar tokens y comparando el desempeño de dichos algoritmos con base en una implementación propia. Zavala et al., describen una simulación de una blockchain haciendo uso de la API Bouncy Castle. Ibarra-García et al., presentan una revisión de la literatura donde comparan distintos enfoques en el uso de contratos inteligentes, sistemas distribuidos y soluciones híbridas que integran blockchain con tecnologías tradicionales de control de acceso. Se presentan algunos desafíos pendientes y las oportunidades

para el desarrollo de sistemas de control de acceso dinámicos y eficientes.

Enseguida, se presentan siete artículos relacionados con avances en el área de la criptografía. Contreras Torres et al., presentan la implementación y validación de un sistema de cifrado de imágenes digitales que combina las técnicas de cajas de sustitución y la de sincronización de autómatas celulares. González Del Río et al., presentan un estudio y aplicación de sistemas caóticos basados en sistemas lineales por pedazos, los cuales pueden ser una gran contribución al cifrado de datos, debido a que estos sistemas son fáciles de implementar y además presentan trayectorias caóticas óptimas para los procesos de cifrado. Padrón-Godínez et al., presentan una mezcla entre implantación de mecanismos de seguridad y fenómenos físicos de propagación para el diseño de un dispositivo ID óptico que contenga información confidencial dentro de un código QR. Ramírez-Torres et al., presentan un criptoanálisis y una propuesta de mejora a un sistema de cifrado basado en un PRBG (Pseudo Random Bit Generator), capaz de generar secuencias binarias utilizando los cuatro estados de un sistema hipercaótico multienroscado. Padrón- Godínez et al., presentan una plataforma de comunicación cifrada implementada en sistemas de logica programable, la cual contiene elementos de transmision y recepción de información además de un mecanismo de cifrado/descifrado para realizar una comunicacion segura. Padrón-Godínez et al presentan una búsqueda de polinomios primitivos para la obtención de los periodos máximos en LFSRs mediante un algoritmo clásico, así como la implementación en dispositivos de lógica programable en VHDL y resultados preliminares mediante simulaciones en cómputo cuántico en la generación de secuencias binarias pseudoaleatorias. Carcaño Ventura et al presentan una visión general sobre lo que es una caja S, esto es, funciones booleanas con un trasfondo matemático complejo. Se explican sus métricas de seguridad y el trabajo de investigación que actualmente se desarrolla.

A continuación, se presentan dos contribuciones en el área de la criptografía postcuántica Delgado Vargas et al., presentan una breve revisión del estado actual que guardan los algoritmos post-cuánticos. De Abiega-L'Eglisse et al., muestran un panorama de las ventajas y los retos de la criptografía post-cuántica en dispositivos de recurso limitado, en escenarios en donde se requiera preservar el servicio de autenticacion.

Finalmente, en el área de redes se presentas dos contribuciones. Arizaga-Silva et al., discuten los antecedentes inmediatos de las redes VANET y establecen los elementos de valor tangibles e intangibles y los activos que hacen de las redes VANET el blanco de ataques cibernéticos. Padrón Godinez describe el diseño e implementación de protocolos de comunicacion con el uso técnicas criptográficas, construyendo eventos donde puede haber vulnerabilidades.

Las RCI4.0 y RCI5.0 han contado con una audiencia de más de 200 personas y 45 diferentes instituciones, entre ellas empresas privadas, centros de investigación universidades e instituciones de seguridad pública. Todos los artículos fueron dictaminados por el comité editorial y revisores expertos en el área.

IMPORTANCIA DE UNA CONFIGURACIÓN SEGURA DE LAS REDES PRIVADAS VIRTUALES (VPN) PARA LA INDUSTRIA 4.0

Sandra Justiniano
Escuela de Ingeniería en Computación
ITCA-Fepade Técnicos e Ingenieros
San Salvador, El Salvador
justiniano.beatriz@gmail.com

Erick Girón
Tecnologías de la Información
Rulesware
Antiguo Cuscatlán, El Salvador
erick.giron89@gmail.com

***Resumen*— La implementación de nuevas tecnologías hace que la demanda de seguridad en la transferencia de información sensible sea indispensable. Constamente se buscan alternativas para el establecimiento de canales seguros, que permitan conectar, por ejemplo, dos sitios remotos. La documentación técnica para configurar una red privada virtual (VPN) es extensa, existen diversos fabricantes que se permiten incluir en sus equipos, los asistentes de configuración, adicionalmente, en internet se puede encontrar información variada, sin embargo, los parámetros incluidos y las consideraciones sobre los servicios de seguridad que se desean proporcionar, muchas veces no son congruentes. Por lo que en este trabajo se propone una configuración que permita cumplir con los estándares de seguridad requeridos actualmente y además se presenta una comparación de la configuración de una VPN con IPsec y los tiempos que toman el envío de paquetes, gracias a la emulación de equipos en GNS3.**

Palabras clave—Industria, IPsec, Seguridad, VPN.

I. Introducción

El diseño de nuevas tecnologías, la automatización de procesos, los servicios en la nube, han permitido el crecimiento de las organizaciones, pero, en consecuencia, esto ha provocado que estas deban preocuparse de mantener el acceso a la información estableciendo conexiones seguras a los servidores y otros [1].

Dado el contexto, el desarrollo industrial no es la excepción; la industria se apoya de los avances tecnológicos, estos influyen directamente en la oportunidad de optimización de procesos, no obstante, la implementación de nuevas tecnologías genera que cada vez se vuelva más compleja la demanda de seguridad en la transferencia de información sensible del negocio, constamente se buscan alternativas para el establecimiento de canales seguros, que permitan conectar, por ejemplo, dos sitios remotos [1] [2].

Las redes privadas virtuales (VPNs), son parte de las herramientas más oportunas para definir un canal seguro, en general, permiten garantizar la autenticación, la confidencialidad y la integridad de los datos transferidos en la comunicación, las alternativas para configurarlas son variadas; los equipos que soporten características criptográficas, fácilmente podrán incorporar licencias para la configuración de una VPN.

Sin embargo, la problemática actual de las comunicaciones, es que no existe mucho énfasis en la implementación de estos canales seguros, y ya que la información es extensa y existen múltiples consideraciones al momento de seleccionar los parámetros que darán soporte a los servicios de seguridad demandados, en algunas ocasiones podrían no estar configurados de la forma más apropiada, mostrando algunas debilidades para los procesos de autenticación o garantías de cifrado e integridad; por lo cual, desde un análisis criptográfico del marco de trabajo de IPsec se propone una guía concreta para la configuración de una VPN.

II. Preliminares

A. VPN

Red privada virtual, representa una tecnología de red que permite conectarse a través de una red pública como una extensión de la red de área local [3], [4].

B. VPN sitio a sitio

Utilizadas para las empresas que desean tener dos o más sitios conectados de forma segura, a través de la red pública, tradicionalmente se emplean el marco de trabajo IPsec para estas implementaciones [5], [6].

C. VPN de acceso remoto

Algunos usuarios requieren una comunicación desde sus computadoras hasta las sedes de la organización, para estas se pueden emplear diversas tecnologías como IPsec o SSL-VPN, y algunas soluciones de diversos fabricantes [5], [6].

D. Industria 4.0

La cuarta revolución industrial es la industria 4.0 que se refiere a la transformación digital aplicada a la industria de producción; precisamente se enfoca en la digitalización de los procesos productivos en las fábricas por medio de sensores y sistemas de información para la transformación en procesos más eficientes [1].

E. IPsec

Es un marco de trabajo de estándares abiertos que garantiza la privacidad de las comunicaciones en Internet. Proporcionando confidencialidad, integridad y autenticidad en las comunicaciones de datos. La principal característica de IPsec es que el tráfico IP puede ser cifrado y/o autenticado, esto se realiza mediante túneles virtuales seguros entre dos pares (peers), por ejemplo, dos routers [5].

F. Confidencialidad

Consiste en la capacidad de garantizar que la información, almacenada o transmitida por la red, estará disponible únicamente para personas autorizadas [5], [7].

G. Integridad

Consiste en garantizar que los datos no han sido modificados sin autorización, por lo cual se puede reconocer que la información de la que se dispone es válida y consistente [5], [7].

H. Autenticación

Consiste en el proceso que un usuario debe completar para tener acceso a los recursos de un sistema o una red, implica la identificación (quién es el usuario) y autenticación (verificar que el usuario sea quien dice ser) [5], [7].

I. Cifrado

Es la práctica de codificar y decodificar datos, aplicando un algoritmo criptográfico, estos utilizan una clave de longitud de bits variable [4], [7].

III. Estado del Arte

Dentro de las tecnologías que permiten la creación de VPN se encuentran las conexiones SSL, redes MPLS, o los túneles IPsec; elegir una o varias de las tecnologías dependerá de las necesidades específicas de la comunicación a realizar y de los recursos disponibles para la implementación; sin embargo, es importante remarcar, que todas estas tecnologías buscan satisfacer las demandas de las redes empresariales. La documentación técnica para configurar una VPN es extensa, existen diversos fabricantes que se permiten incluir en sus equipos, los asistentes de configuración, adicionalmente, en internet se puede encontrar información variada.

En la configuración de las VPN sitio a sitio, Cisco, para las VPN configuradas en Router, sugiere la utilización del grupo de Diffie-Hellman (DH) 2, algoritmo DES para el cifrado, y para garantizar la integridad MD5 [8]; sin embargo, ofrece también un método más fuerte que implica la utilización de SHA-1 para la integridad, certificados digitales con RSA para la autenticación, el algoritmo AES con clave de 128, 192, o 256 para el cifrado y grupos de DH 14 y 24 [5]; Sonicwall sugiere la utilización del grupo de DH 14, y para los procesos de autenticación y cifrado se utilice el algoritmo AES con llaves de 128, 192 o 256 bits [9]; Checkpoint presenta una guía de configuración en donde se utilizan certificados digitales para la autenticación, el algoritmo AES con clave de 256 bits para el cifrado, y SHA-1 para la integridad [10]; Microsoft Azure, ofrece la orientación para la configuración de las políticas de IPsec utilizando AES con claves de 256 para el cifrado, SHA-256 para la integridad y grupos DH 24 [11], [12]; Fortinet, el asistente de configuración contiene una plantilla predefinida, en donde únicamente se solicitan los parámetros de red para establecer el túnel [13].

Dado que existen múltiples tecnologías para la creación de VPNs, se puede identificar que el marco de trabajo IPsec proporciona flexibilidad al momento de configurar un determinado tipo, y con parámetros que permiten satisfacer las necesidades de seguridad oportunas a la comunicación.

IV. Desarrollo de la Investigación

IPsec emplea diferentes métodos para la protección de los datagramas IP, entre los cuales se identifican: autenticación del origen de datos, autenticación de la integridad de los datos sin conexión, confidencialidad del contenido del datagrama, protección anti-reproducción. De acuerdo ello, IPsec se apoya de diferentes herramientas criptográficas para cumplir con los servicios de seguridad especificados.

- Proveer integridad, por medio de funciones Hash y HMAC.
- Combinación de autenticación y cifrado de datos (algoritmos de cifrado y funciones Hash - HMAC).
- Función de intercambio de claves por medio del protocolo Diffie-Hellman (DH).

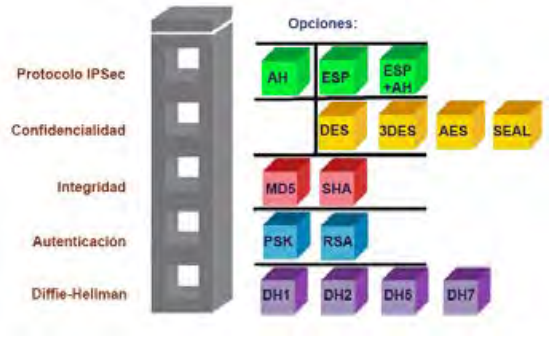


Figura 1. Marco de trabajo IPsec y sus opciones.

Para configurar correctamente una VPN es importante conocer los conceptos asociados a los parámetros que permitirán definir las políticas de seguridad y los mecanismos para el manejo de los paquetes:

- Intercambio de claves de sesión: en el intercambio de las claves de sesión se hace uso del protocolo criptográfico Diffie-Hellman (DH) que permite establecer el *secreto compartido*. DH cuenta con al menos los siguientes grupos: DH1, DH2, DH5, DH14, DH15, DH16, DH19, DH20, DH21, DH24. Los grupos 1, 2 y 5 se considera que no proveen el nivel de seguridad apropiado ante las amenazas más recientes, por tanto, no debe ser utilizado para la protección de información sensible. Si se aplica para la autenticación o cifrado, algoritmos con llaves de 128 bits se utilizan los grupos 5, 14, 19, 20 o 24; si se aplica para la

autenticación o cifrado, algoritmos con llaves de 256 bits o mayores, se utilizan los grupos 21 o 24.

- Integridad y autenticidad de los datos: al garantizar la integridad de los datos se hace uso de los mensajes resumen de los datos del paquete original que viaja con IPsec; estos mensajes se obtienen al aplicar funciones HASH, más específicamente en su construcción con HMAC, pudiendo ser HMAC-MD5 o HMAC-SHA. Por su parte MD5 proporciona un resumen del mensaje con un tamaño de 128 bits, mientras que SHA produce un resumen de 160 bits. MD5 no se considera seguro ya que ha sido vulnerado.
- Método de autenticación de dispositivos: Los extremos involucrados en establecer la comunicación segura por medio de IPsec deben utilizar el protocolo IKE para que, por medio de un proceso de negociación se defina el método para autenticar que se utilizará. Los métodos normalmente aplicados para autenticar son las claves pre-compartidas, haciendo uso de funciones HASH; y la autenticación por medio de firmas RSA, en donde cada extremo firma digitalmente un conjunto de datos, utilizando una autoridad certificadora para otorgar un certificado digital único.
- Cifrado de datos: permite proporcionar confidencialidad, se obtiene empleando algoritmos de cifrado simétricos y claves de sesión. Los algoritmos de cifrados más comunes son: DES, con una clave de 56 bits, 3DES con una clave de 168 bits, y AES con claves de 128, 192 y 256 bits. La seguridad que proporciona un algoritmo recae en la longitud de su clave, por lo cual es recomendable el uso de AES.

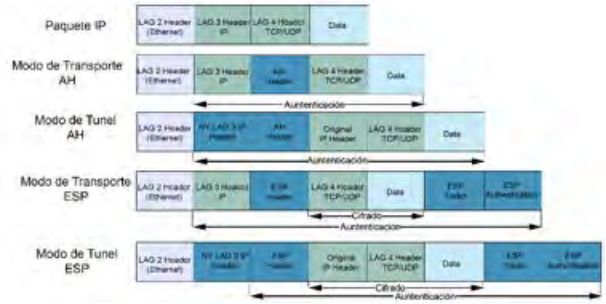


Figura 2. Modos y Encapsulación en IPsec.

Como una guía general, para la definición de una VPN sitio a sitio, se requieren seis pasos.

1) En la fase 1 se requiere crear una política de ISAKMP (Internet Security Association and Key Management Protocol): define los procedimientos de las asociaciones de seguridad (SA – Security Associations), estas contienen la información requerida para la ejecución de servicios de seguridad a nivel de capa de red.
2) Crear llave pre-compartida: es una cadena de texto utilizada en los procesos de autenticación.
3) Crear perfil de ISAKMP: contiene las especificaciones para el manejo de la carga útil del paquete IP.
4) En la fase 2 se requiere definir el set de transformación: contiene la combinación de las transformaciones individuales que tienen lugar en IPsec, cada una para activar las políticas de seguridad específicas para el tráfico.
    a) Un mecanismo para la autenticación de la carga útil (AH transform – permite proveer autenticación e integridad).
    b) Un mecanismo para el cifrado de la carga útil (ESP transform – permite proveer confidencialidad, autenticación e integridad).
    c) Un modo de IPSec, (Modo túnel, se utiliza habitualmente para el cifrado de tráfico en las VPN seguras de IPsec, este modo cifra tanto la carga útil, del paquete, como el encabezado; o Modo transporte, se utiliza únicamente para cifrar la carga útil del paquete, dejando los encabezados intactos).
5) Crear perfil de IPsec.
6) Crear las interfaces túnel y vincular con el perfil de IPsec.

CUADRO I. ALGORITMOS Y FUNCIONES DISPONIBLES PARA ENCABEZADOS DE AH Y ESP

Característica	**AH**	**ESP**
Integridad	MD5 SHA	MD5 SHA
Autenticación	HMAC-MD5 HMAC-SHA1 AES128-XCBC-96	HMAC-MD5 HMAC-SHA HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512 AES-XCBC-MAC
Anti-reproducción	Números de secuencia HMAC-MD5	HMAC-MD5
Confidencialidad	Texto plano	DES 3DES AES AES-CBC AES-CTR
Protección campos de la cabecera	Túnel	Túnel
Modalidad	Túnel Transporte	Túnel Transporte

V. EXPERIMENTOS Y RESULTADOS

Dado que se cuenta con múltiples posibilidades para la configuración de una VPN con IPsec, en diferentes equipos, marcas y asistentes de configuración, se presentan dos

estructuras, en las cuales se han seleccionado determinados algoritmos para los servicios de seguridad especificados, también se muestran los resultados referentes a los tiempos de respuesta de los paquetes; para las pruebas se utilizaron IOS de equipos Cisco emulados en GNS3.

CUADRO II. CONFIGURACIÓN 1

Fase 1					
Autenticación	AES128				
Integridad	MD5				
Grupo Diffie Hellman	14				
Fase 2					
Autenticación	DES	3DES	AES128	AES256	AES256
Integridad	MD5-HMAC	MD5-HMAC	SHA1	SHA256	SHA512
Tiempo Promedio en echo request (ms)	56.2	57.4	55.2	60.2	57.6

CUADRO III. CONFIGURACIÓN 2

Fase 1					
Autenticación	AES256				
Integridad	SHA512				
Grupo Diffie Hellman	24				
Fase 2					
Autenticación	DES	3DES	AES128	AES256	AES256
Integridad	MD5-HMAC	MD5-HMAC	SHA1	SHA256	SHA512
Tiempo Promedio en echo request (ms)	57	58.8	60.8	57.8	60

CUADRO IV. CONFIGURACIÓN RECOMENDADA

Fase 1	
Autenticación	AES256
Integridad	SHA256
Grupo Diffie-Hellman	14
Fase 2	
Autenticación	AES256
Integridad	SHA256

De acuerdo al análisis realizado en las configuraciones de las VPN con los parámetros de los cuadros I y II, y de las características de los algoritmos criptográficos se sugiere la utilización de los parámetros mostrados en el cuadro III, ya que se provee mayor garantía en los procesos de cifrado, autenticación e integridad.

Se sugiere seleccionar modo Túnel, para asegurar todo el contenido del paquete, desde su encabezado; y como protocolo de IPsec ESP, para garantizar el cifrado de la carga útil.

VI. CONCLUSIONES

La robustez de la configuración de una VPN se encuentra directamente vinculada a las características de los principales algoritmos de cifrado, de acuerdo a su modo de operación y la longitud de llaves implementadas; IPsec sugiere el tipo de algoritmos a incluir según el servicio de seguridad que desea gantizarse.

La disponibilidad de ciertos algoritmos y longitudes de llaves están vinculados, también, a las características criptográficas incluidas en los sistemas operativos de los diferentes dispositivos, considerando además las recomendaciones de los fabricantes.

Los resultados del escenario implementado demuestran que las diferencias en RTT (Round-trip time), para los diferentes modos de configuración en la creación de VPNs IPSec entre dos pares, son despreciables así, al contrastar velocidad de cifrado versus fortaleza de los algoritmos a utilizar, es este último factor el más importante a tomar en cuenta al diseñar un túnel VPN IPSec.

Es importante mencionar que la interoperabilidad entre diferentes marcas de equipos conlleva la utilización de diferentes combinaciones de algoritmos y funciones que son parte del marco IPsec, por lo cual es necesario comprender las características principales de cada uno de ellos.

VII. RECOMENDACIONES

Utilizar algoritmos de cifrado y funciones HASH más fuertes y que no hayan sido vulnerados.

Se recomienda la utilización de claves con la mayor longitud posible, para garantizar la fortaleza del cifrado.

Determinar los servicios de seguridad que se requieren garantizar con la configuración de la VPN IPsec, y seleccionar los algoritmos y funciones mas robustos posibles.

Consultar las recomendaciones del fabricante, verificando además las características incluidas en los sistemas operativos de los dispositivos.

Realizar pruebas de la configuración de la VPN con IPsec, e identificar posibles ataques en un entorno controlado, previo a la implementación.

REFERENCIAS

[1] ISOTools, “Industria 4.0: ¿Cuál es la importancia de la estandarización?” Disponible en: https://www.isotools.org/2018/06/13/industria-4-0-estandarizacion/ Junio 2018 [Accedido: Septiembre 29, 2018].

[2] Cluster Industrial, “Ciberseguridad un reto para la Industria 4.0”. Disponible en: https://clusterindustrial.com.mx/post/3566/ciberseguridad-un-reto-para-la-industria-4-0/ Marzo 22, 2018 [Accedido: Septiembre 29, 2018].

[3] L. Cornett, K. Grewal, M. Long, M. Millier, S. Williams, “Network Security: Challenges and Solutions”, Intel® Technology Journal, vol. 14, no. 2, 2009.

[4] W. Odom CCNA, S. Hogg, Routing and Switching, ICND2 200-105 Official Cert Guide, Indianapolis, IN: Cisco Press, 2017.

[5] O. Santos, J. Stuppi, CCNA Security 210-260 Official Cert Guide, Indianapolis, IN: Cisco Press, 2015.

[6] Cisco Networking Academy, “CCNA Routing and Switching: Conexión de Redes v6”, Disponible en: https://www.netacad.com/ 2018 [Accedido: Septiembre 29, 2018].

[7] A. Menezes, P. van Oorschot, S. Vanstone. (1996). Overview of Cryptography. En Handbook of Applied Cryptography(5). CRC Press: CRC Press, Inc.

[8] Cisco Engineers, “Configuration Professional: Site-to-Site IPsec VPN Between Two IOS Routers Configuration Example”. Disponible en:

https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/configuration-professional/113337-ccp-vpn-routerA-routerB-config-00.html/ Noviembre 30, 2011 [Accedido: Agosto, 2018].

[9] Sonicwall, “How to Configure a Site to Site VPN Policy using Main Mode”. Disponible en: https://www.sonicwall.com/en-us/support/knowledge-base/170504380887908/ Mayo 11, 2018 [Accedido: Agosto, 2018].

[10] Checkpoint Software Technologies, “How to Set Up a Site-to-Site VPN with Check Point Gateways Managed by the same Management Server”. Disponible en: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk54060/ Marzo 6, 2018 [Accedido: Agosto 2018].

[11] Microsoft Azure, “Create a Site-to-Site connection in the Azure portal”. Disponible en: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal/ Marzo 4, 2018 [Accedido en: Agosto 2018].

[12] Microsoft Azure, “Configure IPsec/IKE policy for S2S VPN or VNet-to-VNet connections”. Disponible: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-ipsecikepolicy-rm-powershell/ Febrero 13, 2018. [Accedido: Agosto, 2018].

[13] V. Martin, “Site-to-site IPsec VPN with two FortiGates” Disponible en: https://cookbook.fortinet.com/site-site-ipsec-vpn-two-fortigates-56/ Enero 10, 2018. [Accedido: Agosto, 2018].

Sistema de control de acceso utilizando tarjetas RFID y reconocimiento de emociones

Diana Carolina Carrión Martínez
Ciencias en Tecnologías de Seguridad
Instituto Nacional de Astrofísica, Óptica y Electrónica
Puebla, México
dianaccmtz@inaoep.mx

Esaú Moisés García Reyes
Ciencias en Tecnologías de Seguridad
Instituto Nacional de Astrofísica, Óptica y Electrónica
Puebla, México
esaumgr@gmail.com

David Gonzalez Martínez
Ciencias en Tecnologías de Seguridad
Instituto Nacional de Astrofísica, Óptica y Electrónica
Puebla, México
david.gonzalez.mtz@gmail.com

***Abstract*—En este documento se presenta un sistema embebido para el control de acceso mediante el uso de tecnología RFID, en conjunto con un módulo de reconocimiento de expresiones faciales el cual tiene la finalidad de identificar emociones en las expresiones del rostro mediante el uso de un algoritmo de procesamiento de imagen. Buscando llevar una supervisión en los horarios y las áreas accesadas, así como las emociones expresadas al momento de ingresar a una zona autorizada ocupando las tarjetas RFID. Esto, con el fin de recabar información que provea datos, los cuales se podrán usar posteriormente para la realización de un análisis estadístico y evaluar el desempeño del personal así como la influencia del estado emocional en el clima laboral y la interacción social.**

***Index Terms*—IoT, Control de Acceso, RFID, Emociones, Reconomiento de Expresiones**

I. Introduction

El registro de acceso controlado en las instalaciones de instituciones privadas y del sector público es un elemento necesario para reforzar los mecanismos de seguridad con los que todo organismo que emplee y conserve a resguardo información sensible debe contar. Por una parte, existe la obligación de que por ley dichas instituciones deben de tratar como confidencial la información que se procesa para los fines que haya sido recabada y por otra parte, para evitar exponerla a usuarios no autorizados e impedir el uso indebido de la misma. Por lo anterior, se precisa contar con registros de ingreso tanto del personal que labora en dichas instituciones, así como de los visitantes y usuarios de servicios que estas ofrecen. La identificación o comprobación de la identidad es el método por el que se han inclinado la mayoría de las empresas. Es por lo mismo que se han creado sistemas de identificación y control, los cuales han ido evolucionando para ofrecer una mayor seguridad, junto con funciones que den soluciones a problemas a la medida de las corporaciones. Para lograr esto se han propuesto diversas formas de identificación como la dactilar, retina, password, palabras clave, tarjetas, identificación, etc. Una de las tecnologías que actualmente se encuentra trazando su camino y la que se ocupara para este sistema es el RFID, la cual es relativamente barata y fácil de ocupar. Los principales retos que enfrentan estas tecnologías son: la mejora en la seguridad, tanto de la empresa como de la misma tecnología usada, debido a que a medida que evolucionan, de igual forma mejora el método para romper dicha seguridad. Así mismo se crean tecnologías que sirven para bloquear o imitar la tecnología utilizada y de esta manera engañar al sistema. Por lo tanto se vuelve necesario buscar nuevas formas de prevenir dichas dificultades y/o mejorar la seguridad en estas. De igual forma existe el problema de las limitaciones en la misma tecnología; en el caso de las tarjetas RFID cuentan tanto con una memoria como con un rango de alcance corto. Esto limita la programación dentro de las mismas tarjetas, entre otras dificultades.

En el caso del módulo de detección de emociones, resulta interesante aprovechar el sistema de control de acceso para obtener un tipo distinto de información que permita realizar estudios posteriores de análisis de conducta empleando las emociones mostradas por los usuarios, lo cual podría ser un factor que contribuya a evaluar aspectos como la interacción de los miembros de una organización, el desempeño y clima laboral. Para lograr esto se usa un programa de reconocimiento de expresiones faciales en conjunto con una cámara. Esta tecnología todavía se encuentra en desarrollo, ya que existen pocos algoritmos los cuales cumplen con dicho cometido de forma satisfactoria. El leer las emociones en los rostros en sí mismo es un reto incluso para los expertos, puesto que existen las micro expresiones, las expresiones falsas o contenidas e incluso personas que no demuestran emociones ya sea por algún problema de salud pasado o presente, los cuales a simple vista son difíciles de identificar. Es por lo mismo que actualmente los métodos existentes no son totalmente confiables y los resultados que presentan los mismos siguen siendo ineficaces.

II. Marco Teórico

El uso de la tecnología RFID actualmente está centrado en el registro de productos a gran escala, para llevar control sobre estos, gracias a que está tecnología es económica, y cuenta con el espacio suficiente para las características básicas de los productos. Aunque ya se empiezan a ver las bondades de esta tecnología para personas, su uso actualmente se encuentra en crecimiento. En uno de los campos donde se está utilizando, mayormente, es en el área hospitalaria, donde se usa para llevar un registro de los pacientes, sus datos y su localización dentro

del edificio. En cuanto al tema de seguridad para la tecnología RFID, existen diversos algoritmos que se encuentran en uso y los cuales no generan un gran costo computacional, un ejemplo de este es el AES, un algoritmo con una fuerte autenticación simétrica y el cual cuenta con la ventaja de un costo de energía bajo y una matriz de tamaño menor. Mientras que dentro de los algoritmos de reconocimiento de expresiones faciales; la mayoría de estos métodos utilizan redes convolucionales profundas, las cuales pueden diferir en el número de capas, el tipo de elementos que usan, así como los componentes de las mismas. Se buscan en estos métodos, enfocarse en las características faciales y los movimientos que realizan para descubrir las emociones proyectadas, y, aunque todavía es un trabajo en proceso y con grandes complicaciones, ha mejorado en el reconocimiento de estos.

A. Identificación por Radio-Frecuencia

RFID (Radio-frequency identification), permite el uso de un objeto (normalmente llamado tag RFID) que se adosa a un producto, animal o persona con el propósito de identificación y seguimiento usando ondas de radio. Un tag RFID consta de dos partes principales: a) un circuito integrado para almacenar y procesar información, modular y demodular la señal de RF y otras funciones especializadas; b) una antena para recibir y transmitir la señal. (Carignano, 2011) [1]. Una de las principales ventajas que se tiene con RFID es que se puede identificar un producto como único, es decir, productos iguales pueden ser diferenciados por una clave contenida en su etiqueta de RFID, a diferencia del código de barras que para productos iguales es el mismo. Una etiqueta de RFID es mucho más complicada de clonar que un código de barras que puede ser igualado por medio de una fotocopia (Alvarado, 2008) [2].

B. Lector RFID-RC522

El módulo RC522 es un lector que genera un campo magnético y que fue desarrollado para comunicarse sin necesidad de contacto con tarjetas y transpondedores sin circuitos activos para leer datos contenidos en ellas. El módulo lector RFID-RC522 RF utiliza 3.3V como voltaje de alimentación y se controla a través del protocolo SPI. También puede ser controlada con un puerto UART. Entonces, podemos decir que es compatible con casi cualquier micro controlador o tarjeta de desarrollo (Orlando, 2014) [3].

C. Expresiones faciales y emoción

En 1993, Ekman señaló que “las expresiones faciales son un componente importante de la conducta emocional y son específicas para las emociones básicas” y en ese mismo sentido, en The Handbook of Cognition and Emotions (2005) afirmó que “la evidencia [sobre la universalidad de las emociones] es más fuerte para la alegría, el enojo, el disgusto, la tristeza y el miedo/sorpresa”. En general, quienes defienden la existencia de emociones básicas asumen que se trata de procesos directamente relacionados con la adaptación y la evolución, que tienen un sustrato neural innato, universal y un estado afectivo asociado único (Chóliz, 2005) [4]. Precisamente, la universalidad de las emociones ha sido demostrada con base en estudios realizados en niños ciegos de nacimiento pues, se ha comprobado que todos los recién nacidos expresan una especie de sonrisa a partir de las cinco semanas de vida, incluso si son ciegos. Los niños ciegos de nacimiento también ríen, lloran, fruncen el ceño y adoptan expresiones típicas de ira, temor o tristeza (Castro y Sámano, 2016) [5].

D. Reconocimiento facial

De acuerdo con (Castro y Sámano, 2016) [5] las tecnologías de reconocimiento facial, se apoyan en disciplinas como el procesado de imagen, redes neuronales, reconocimiento de patrones y visión por computadora y tienen como objetivo conseguir que dada una imagen de una cara desconocida (o imagen de test) se pueda encontrar una imagen coincidente con la misma en un conjunto de imágenes conocidas (conjunto de entrenamiento). Sin embargo, este proceso de clasificación no es lo de mayor prioridad al momento de llevar a cabo el reconocimiento de rostros pues “la clasificación es menos importante, ya que esta se encuentra integrada en el proceso de detección; es decir, nosotros queremos detectar cambios de manera precisa los cuales son importantes para reconocer emociones” (Martínez y Du, 2012) [6]. En ese sentido, debe comprenderse que para poder llevar a cabo el análisis de emociones con base en gesticulaciones del rostro, y como ha sido mencionado en Álvarez y Guevara (2009) [7] “la mayoría de investigaciones que realizan el reconocimiento de expresiones faciales parten del hecho que se tiene la región del rostro previamente detectada” por lo tanto, la prioridad es desarrollar sistemas capaces de identificar los cambios más sutiles en el semblante a fin de extraer correctamente las características emocionales que lo definen.

III. Problema

Actualmente las empresas tienen problemas con la filtración de datos, fuga de información y robos de equipos que se encuentran en desarrollo o que ya están proximos a ser presentados al público, estos fallos de seguridad pueden causar a la empresa grandes problemas tanto económicos como de innovación y de patente, lo que también le da a sus adversarios ventaja sobre los mismos, lo cual puede significar un fuerte revés para su posición en el mercado, si no su supervivencia en el mismo. En caso de información sensible en instituciones publicas el robo o fuga de estas puede llegar a causar daños a las instituciones y el personal que trabaja para ellas, junto con una pérdida en la confiaza de la misma. Y aunque lo ideal es un sistema infalible y 100% seguro, esto no es posible ya que siempre se encontrarán agujeros y fallos en el. Por lo tanto se busca tener distintas medidas de seguridad para lograr obtener un sistema con un mejor control y prevenir en la medida de los posible las perdidas. La prevención es lo que juega un papel importante y es la mejor opción para las empresas que buscan mantener sus activos seguros y que la probabilidad de fugas o robos disminuya. Para esto se busca controlar el acceso y llevar un registro muy estricto de lo que cada empleado puede

hacer dentro de la empresa y a donde estos pueden acceder dentro de la misma.
Además de exportar diversa información sobre la asistencia del personal y usuarios para la toma de decisiones, las cuales pueden tener consecuencias inmediatas en el caso de los clientes que conlleven a una pérdida del trabajo. [8]

IV. Desarrollo

Se utilizó una base de datos para guardar los registros de los empleados y la información que posteriormente se creará. Analizando el ambiente y las necesidades de la empresa se crearon las tablas y sus relaciones, las cuales quedaron abiertas a posibles cambios por sí la empresa así lo requería. Para la creación de la interfaz gráfica así como la programación se utilizó Python, ya que este lenguaje actualmente cuenta con una gran comunidad que lo mejora de forma constante, y por lo mismo se encuentra en constante cambio y con un gran equipo que le da soporte casi diariamente. Para la lectura de las tarjetas RFID se utilizó un lector RFID, así mismo se ocupó un keypad para la introducción de una contraseña, la cual se espera el usuario proporcione después de pasar su tarjeta, y que esta sea correctamente autorizada por el mismo sistema.
Tanto el lector como el keypad se conectan a un arduino elegoo mega 2560, el cual a su vez se conecta a un módulo wifi, el cual envía la información encriptada, tanto de la tarjeta como del password del empleado a una computadora receptora, la cual guarda la información. Para la programación de estos componentes y la obtención de datos de la tarjeta junto con la conversión de la misma a un lenguaje que la base de datos pueda comprender se utilizó el lenguaje de programación de Arduino es C++. No es un C++ puro sino que es una adaptación que proveniente de avr-libc que provee de una librería de C de alta calidad para usar con GCC (compilador de C y C++) en los microcontroladores AVR de Atmel y muchas utilidades específicas para las MCU AVR de Atmel. Una vez creado el vínculo con la base de datos y el arduino se usó programación multihilos para que no hubiera necesidad de estar reiniciando el programa para el registro de los empleados, los datos de los empleados se muestran en una pantalla, obsérvese la figura 1.

Para la programación de las emociones se investigó primero los algoritmos existentes y cuales tenían mejores resultados para una cámara no tan potente, resultando el clasificador Naive Bayes, k-NN, SMV y Multilayer Preceptron. Se utilizo python para la programación de este clasificador, aunque en esta ocasión se utilizo Python3 para mejores resultados. Para crear el programa de reconocimiento se utilizo TFlearn sobre Tensorflow y distintos módulos junto con bases de datos de imágenes para su posterior entrenamiento, ya implementado y funcionando el reconocimiento se puede observar en la figura 2.

A continuación, en la figura 3, se podrá observar el diagrama básico del sistema de control. Donde se podrá observar, el módulo wi-fi, el cual enviará la información al sistema de control central y la base de datos. El lector de tarjetas RFID, así como el keypad donde el usuario insertará su clave de acceso y un buzzer, el cual sonará cuando la tarjeta sea reconocida, de igual manera cuando el password sea validado.

Fig. 1: Datos del empleado

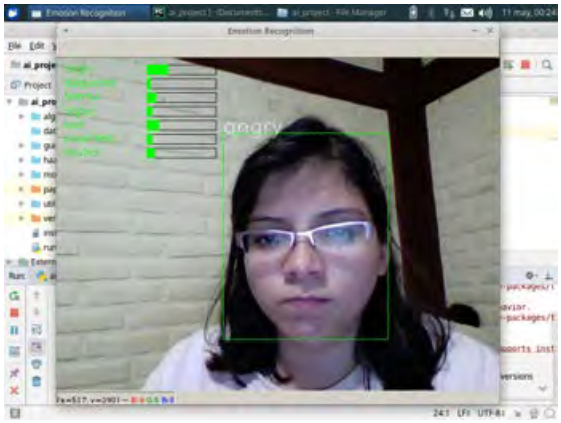


Fig. 2: Reconocimiento de emociones

V. Conclusiones

El desarrollo y optimización de los equipos en las empresas es necesario para eficientar los procesos y llevar un mejor control de los datos que la empresa genera. La seguridad invertida para proteger los bienes debe ser cada vez mayor, puesto que aun cuando la información almacenada no contenga datos sensibles puede acarrear cierto peligro para las organizaciones. Por lo mismo es necesario que tanto los fabricantes de tecnologías así como las empresas mismas se aseguren que estas tengan algún método de seguridad implementado.
Esto en conjunto ayuda a que se ahorren tanto problemas como gastos, junto con un mejor almacenamiento de la información y optimización en los procesos. La utilización de las tarjetas

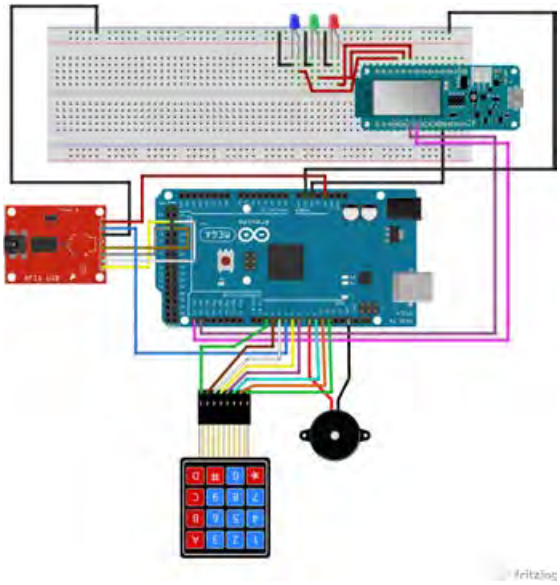


Fig. 3: Diagrama Fritzing

RFID ayuda que la persona pueda llevar sus datos en cualquier momento y se pueda identificar dentro de la empresa de forma sencilla y sin la necesidad de algún complemento extra ya que esta tecnología es liviana y fácil de usar. De igual manera, es necesario monitorizar a los empleados, así como el estado de ánimo en el que se encuentran puesto que, la producción de estos depende del mismo. Cuando un empleado no es feliz en su área de trabajo, su productividad baja, o si existe algún tipo de inconformidad puede realizar acciones que dañen directa o indirectamente a la empresa. Por lo cual, reconocer y prevenir estas emociones, entre otras, es algo de vital importancia para las empresas.

VI. Bibliografía

References

[1] Alvarado Sánchez, J., Sistema de Control de Acceso con RFID. Tesis para obtener el grado en Maestro en Ciencias en la especialidad de Ingeniería Eléctrica Opción Computación, Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional, México, 2008

[2] Carigniano, M. F. y Ferreyra, P. Tecnología Inalámbrica Near Field Communication y sus Aplicaciones en sistemas embebidos. En: Congreso Argentino de Sistemas Embebidos, (2 – 4, Marzo). Buenos Aires Argentina. p. 97.

[3] Orlando, (2014). Módulo RFID-RC522 RF con Arduino UNO SPI. Recuperado de: https://hetpro- store.com/TUTORIALES/modulo- lector- rfid-rc522- rf- con- arduino/

[4] Mariano Chóliz (2005): Psicología de la emoción: el proceso emocional. Recuperado de: www.uv.es/=choliz/Proceso

[5] Castro Reyes, JC. y Sámano Rodríguez, JG. (2016). Reconocimiento de microexpresiones utilizando PCA. Tesis para obtener el título de Ingeniero en Comunicaciones y Electrónica. Instituto Politécnico Nacional. Escuela superior de ingeniería mecánica y eléctrica, unidad profesional;Adolfo López Mateo; México, D.F.

[6] Martínez, A. y Du, S. A model of the Perception of Facial Expressions of Emotion by Humans: Research Ovierview and Perspectives. National Institute of Health Public Access. J Mach Learn Res. 2012 May 1; 13: 1589–1608.

[7] Álvarez, D. y Guevara, M. Reconocimiento de expresiones faciales prototipo usando ICA. Scientia et Technica Año XV, No 41, Mayo de 2009. Universidad Tecnológica de Pereira. ISSN 0122-1701.

[8] Sistemas de control de accesos para empresas: ¿cuándo es necesario?: http://blog.fermax.com/esp/sistemas-de-control-de-accesos-para-empresas-cu%C3%A1ndo-es-necesario

Diseño de sistema automático de alineación de cámaras mediante triangulación

Julio A. Grajales-Flores
Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE), Laboratorio de Visión por Computadora
Puebla, México
jagrajales@inaoep.mx

Gabino Martínez-Cruz, Manuel G. Espinoza-Hernández
Secretaría de Marina, GTT Garfio3
CDMX, México
gabino_martinez@semar.gob.mx, mgespinoza@semar.gob.mx

***Resumen*—En estos días, los sistemas de seguridad de armas modernos requieren de una alta precisión, por lo cual, el diseño de aplicaciones más eficientes es requerido. En este trabajo de investigación se describe la implementación y aspectos de seguridad de un esquema que realiza la alineación automática de un arreglo de cámaras, con base en la triangulación de objetos para obtener una alineación muy precisa entre el director de tiro y el montaje. De acuerdo a los resultados obtenidos, el prototipo desarrollado puede considerarse como una buena alternativa para aplicaciones de alineación, así mismo se consideró la integración de servicios de autenticación, confidencialidad e integridad para incrementar la seguridad.**

***Index Terms*—Alineación, Seguridad, Hardware, Automatización, Triangulación, Directores de tiro.**

I. Introducción

El término *Sistema de armas* es una generalización que comprende un amplio espectro de componentes y subsistemas, los cuales varían desde simples dispositivos ofensivos/defensivos y plataformas de lanzamiento, que pueden ser de una clase diferente de acuerdo al buque o unidad flotante que se tome como referencia, en términos generales, haremos referencia a esta expresión como la integración de un sistema de control de tiro y uno o varios cañones (figura 1).

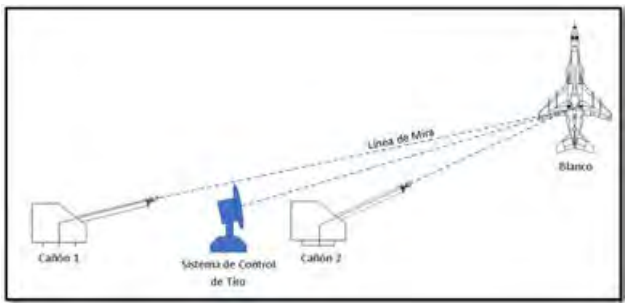


Figura 1. Representación de un sistema de armas compuesto por 2 cañones y un sistema de control de tiro.

Se le denomina *cañón*, a la pieza mecánica que es capaz de eyectar una munición o dispositivo explosivo con fines de disuasión, defensa o ataque, el cual se encuentra montado sobre la superficie plana de un buque. Esta conformado de diferentes partes, siendo la boca de fuego una de las más importantes, porque desde esta pieza es eyectada la munición (figura 2).

Figura 2. Representación de un cañón con su boca de fuego.

La eficiencia de los sistemas de armas dependen de varios aspectos, sobre todo del tipo de sistema al que se haga referencia. En este caso, en específico se hará alusión a un sistema de armas consistente en una pieza de artillería conocido como montaje (cañón) y un director de tiro electro-óptico (figura 3), estos componentes trabajando en conjunto tienen una eficiencia de tiro promedio del 80 %, este valor depende de varios factores como: el cálculo balístico, la dispersión del montaje, la capacidad del director de tiro para la adquisición, filtrado y traqueo de blancos, así mismo dependerá de la alineación del sistema de armas. Todos estos factores influyen en igual escala, por lo que es necesario asignarles el mismo nivel de importancia, ya que todos son dependientes unos de otros.

En este trabajo, se presenta en forma general la implementación de un prototipo para llevar a cabo el método de alineación de un sistema de armas. El objetivo de esta aplicación es realizar una alineación muy precisa entre el director de tiro y el montaje. Por otro lado se mencionan algunos aspectos relevantes de seguridad que pueden implementarse para mejorar el sistema como manejo de llaves y protocolos de comunicación. Este tema es de vital importancia, ya que cada vez, mejores sistemas de seguridad en armas son requeridos. Por otro lado, para que los disparos acierten sobre el blanco, los sistemas

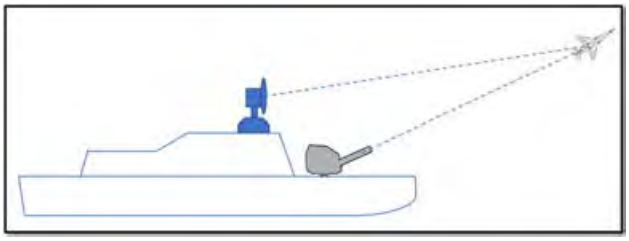


Figura 3. Representación de una alineación dinámica, considerando un Director de Tiro y un Cañón.

requieren un alto grado de precisión. Actualmente, algunos métodos para realizar la alineación de sistemas de armas, se basan en la utilización de miras telescópicas y teodolitos, pero ambos anteponen como requisito que el buque se encuentre en seco (en dique), para que la alineación pueda llevarse a cabo de manera precisa. Estos métodos son tardados y costosos por el procedimiento que conlleva poner un buque en seco.

II. Alineación

En un escenario real, tanto el sistema de control de tiro, como los cañones deberán estar apuntando al blanco en el mismo punto, para poder llegar a efectuar esto, es necesario realizar un ejercicio que asegure la convergencia de la mira de estos elementos. Por consiguiente, la alineación, es un proceso que debe llevarse a cabo en los sistemas de armas. Además, debe ejecutarse como parte de la integración y puesta a punto para la correcta operación de dicho sistema. Por otro lado, la inexactitud de la alineación ocasionará que, en alguno de los módulos, su línea de mira este observando un punto diferente al requerido, ocasionando con esto, una mala lectura y a su vez, una mala ejecución del problema [8].

La alineación estática consiste en colocar un cañón y un sistema de control de tiro, en planos paralelos, respecto a un punto de referencia, el cual, normalmente es un equipo externo al sistema de armas, llamado giroscópica. Los tres planos (x, y, z) de cada sistema, son comparados con las lecturas de los planos del equipo de referencia, esta medición generará un valor de error, el cual será agregado en los módulos respectivos para compensar esa diferencia, consiguiendo así que todos los módulos estén referenciados al mismo punto [11].

La alineación dinámica es en la que se enfoca este trabajo. Este proceso se lleva a cabo una vez que fue efectuada la alineación estática y consiste en colocar a punto la línea de mira de cada uno de los elementos del sistema de armas, considerando un punto de referencia a cierta distancia. Tomando como base la alineación anterior, los puntos de vista de cada módulo no deberán estar muy desfasados, sin embargo, para garantizar un ajuste fino, se ejecuta esta alineación, consiguiendo eliminar los errores mínimos que puedan existir. Normalmente se posiciona un blanco fijo a línea de vista a una distancia de tres kilómetros, para así hacer converger las líneas de mira de cada uno de los módulos [12].

III. Método de alineación por tringulación

La problemática que se requiere resolver con el desarrollo del equipo de alineación dinámica de cámaras por triangulación, consiste en realizar la alineación del armamento con el buque a flote en amarras con el fin de disminuir los tiempos y costos de los métodos de alineación usados actualmente a bordo de los buques, al dejar de ser una condicionante que el buque se encuentre en dique. Además, este método permite mejorar la alineación del armamento e implícitamente mejorar la eficiencia de los sistemas de armas.

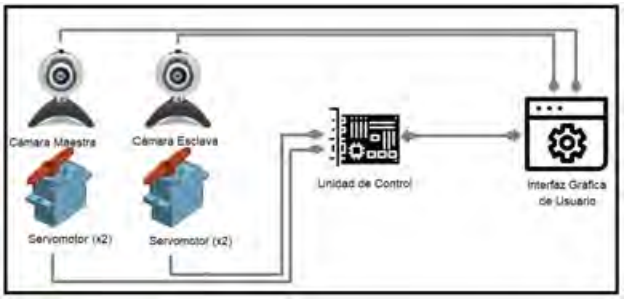


Figura 4. Diagrama del sistema de alineación propuesto.

En la figura 4, se muestra el diagrama a bloques de los componentes que conforman el prototipo del sistema de alineación dinámica, se presenta la integración de sensores (cámaras), actuadores (servomotores), unidad para controlar los servomotores (tarjeta de control) y la interfaz gráfica de usuario ejecutándose sobre una PC portátil, que proporciona un entorno visual sencillo para ingresar y obtener datos de la unidad de control.

En el prototipo, se desarrolló un algoritmo de triangulación en una tarjeta arduino y una interfaz de usuario, en la cual se puede administrar el control de los cuatro servomotores, los cuales están instalados en dos brazos mecánicos de un sistema pan & till con movimientos rotativos en el eje horizontal y vertical (elevación), donde se instaló una cámara web en cada brazo mecánico, con la finalidad de simular los movimientos del director de tiro y el cañón de un sistema de armas. Los ejes ópticos de las cámaras web simulan la línea de mira, correspondientes a las cámaras de un director de tiro electro-óptico y a la línea de mira de la boca de fuego del cañón. El método que se propone consiste en posicionar el eje óptico de una cámara web, montada sobre un brazo robotizado (cámara maestra) visualizando un blanco en el horizonte, se obtienen los ángulos del eje vertical y horizontal del brazo mecánico, siendo necesario realizar telemetría, para conocer la distancia existente entre el eje óptico de la cámara maestra y el blanco simulado. El valor de la distancia medida se introducirá a la interfaz gráfica de usuario desde donde se enviará por puerto serial USB, el dato a la unidad de control para realizar los cálculos de triangulación y obtener los ángulos del posicionamiento del eje vertical y horizontal del brazo mecánico de la cámara esclavo, mostrando en la interfaz gráfica, el valor de los ángulos del problema solucionado y

comparando que las imágenes se encuentran focalizando el mismo punto en el horizonte, asimismo el sistema será capaz de realizar los cálculos matemáticos para corregir el valor de la distancia longitudinal y altura que existen entre los ejes de giro de los brazos mecánicos, donde se encuentran instaladas las cámaras [2].

III-A. Ecuaciones implementadas para resolver el problema de triangulación

a) $El_{c,m}$ = Elevación Cámara Maestro
b) $Rz_{c,m}$ = Ronza de Cámara Maestro
c) $Do_{c,m}$ = Distancia del objetivo desde la Cámara Maestro
d) $Ez_{c,e}$ = Ronza Cámara Esclavo
e) $El_{c,e}$ = Elevación Cámara Esclavo
f) $D_{c,e}$ = Distancia del objetivo desde la Cámara Esclavo
g) Dh = Componente Horizontal
h) $A_{e,m}$ = Altura Cámara Esclavo con respecto a Cámara Maestro
i) $L_{e,m}$ = Longitud Cámara Esclavo con respecto a Cámara Maestro
j) $X_{c,m}$ = Componente en X de la Cámara Maestro
k) $Y_{c,m}$ = Componente en Y de la Cámara Maestro
l) $Z_{c,m}$ = Componente en Z de la Cámara Maestro
m) $X_{c,e}$ = Componente en X de la Cámara Esclavo
n) $Y_{c,e}$ = Componente en Y de la Cámara Esclavo
o) $Z_{c,e}$ = Componente en Z de la Cámara Esclavo

Cuadro I
VARIABLES UTILIZADAS EN EL PROCESO DE TRIANGULACIÓN.

III-B. Procedimiento para realizar la triangulación y corrección de la alineación

Considerando que el director de tiro y el montaje en un escenario real se encuentran en diferentes distancia longitudinal y altura, se tomó esta idea como base para colocar las cámaras en posiciones diferentes para simular ese entorno, a continuación, se miden los datos de las variables h), i), despúes se posiciona el eje óptico de la cámara maestra visualizando un punto objetivo de referencia para determinar los datos de a), b), con esa información se calcula la distancia existente de la cámara maestra al punto de referencia c) (Cuadro I). Después se realiza el cálculo de las siguientes ecuaciones para conocer el valor de las variables y realizar la tringulación (Cuadro II).

$D_h = D_0 cos(El_{c,m})$
$X_{c,m} = D_h cos(RZ_{c,m})$
$Y_{c,m} = D_h sen(RZ_{c,m})$
$Z_{c,m} = D_0 sen(El_{c,m})$
$X_{c,e} = X_{c,m} - (L_{e,m})$
$Y_{c,e} = Y_{c,m}$
$Z_{c,e} = Z_{c,m} - A_{p,d}$
$D_{c,e} = \sqrt{X_{p,a^2} + Y_{p,a^2} + Z_{p,a^2}}$
$RZ_{c,e} = tan^{-1}(\frac{Z_{c,e}}{D_{c,e}})$

Cuadro II
ECUACIONES IMPLEMENTADAS PARA RESOLVER EL PROBLEMA DE TRIANGULACIÓN.

IV. RESULTADOS

IV-A. Caso de prueba

Para este caso, se proyectó sobre una superficie la imagen de un helicóptero como objetivo designado, posteriormente se calculó la distancia hacia el objeto, haciendo uso de un medidor láser. La figura 5 muestra la Interfaz Gráfica de Usuario con los datos de la primera aproximación, de lado izquierdo se presenta la visión de la cámara principal apuntando a la parte inferior de la imagen del helicóptero, del lado derecho se presenta la visión de la cámara secundaria, donde se puede apreciar que no está alineada tomando como base la imagen de la izquierda.

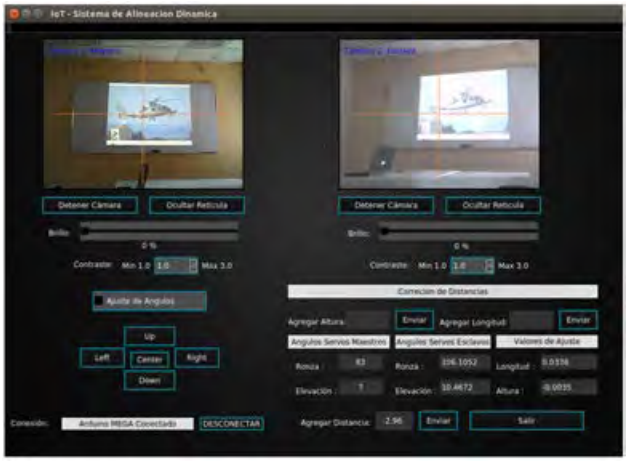


Figura 5. Caso de prueba sin corrección.

Tal como se muestra en la figura 5, el conjunto de servos esclavos, no apuntó directamente a donde estaba el objeto, esto debido a que la distancia del objeto aun no era conocido, como paso a seguir, es la identificación del objeto. Para nuestro caso, su distancia es de 3.52m, la cual se obtuvo al hacer uso de un telémetro láser, una vez agregado ese dato, la solución se muestra en la figura 6, donde se aprecia que la visión de ambas cámaras se encuentra alineada.

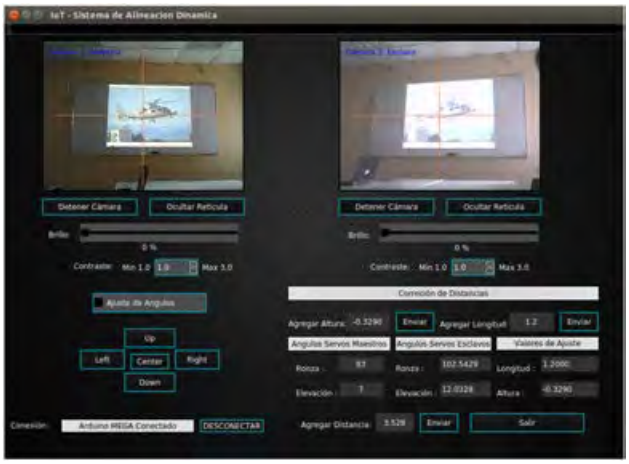


Figura 6. Caso de prueba con corrección.

Aunque visualmente se puede percibir que la corrección es exacta, se corroboró la información haciendo uso de la

herramienta Matlab, donde la simulación arrojó la gráfica que se observa en la figura 7. La etiqueta *Maestro* indica la posición de la cámara principal y la etiqueta *Esclavo* indica la posición de la cámara secundaria, la cual se encuentra a diferente distancia longitudinal y altura, la línea en azúl que recorre el eje x indica el eje óptico de la cámara maestra, la cual se intersecta con la línea roja que representa el eje óptico de la cámara esclava, se puede concluir que el eje óptico de ambas cámaras se encuentran alineadas al objetivo designado.

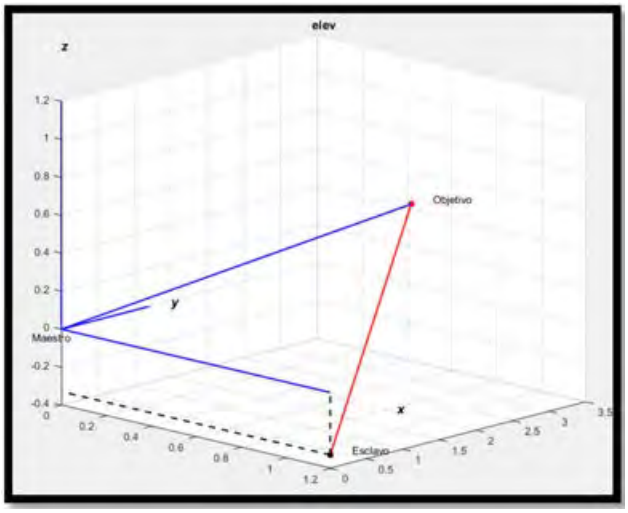


Figura 7. Simulación del caso de prueba.

Con ello se corrobora que los cálculos efectuados son correctos, tanto en la simulación como en la implementación de la interfaz, en conjunto con el control de los servos.

Como se pudo apreciar en la prueba anterior, el resultado fue preciso, considerando distancias, posiciones y ángulos, corroborando estos resultados a través de la simulación en Matlab.

Algunas de las limitaciones identificadas en este prototipo, es la precisión en el ensamble de los brazos mecánicos, los cuales no están bien rectificados, lo que puede ocasionar un desfase en lo que realmente están viendo las cámaras, puesto que nuestra primera consideración es que las cámaras estén posicionadas en un punto 0,0,0 para las coordenadas de X, Y y Z. La solución, es un ensamble con tolerancias más precisas. Otra de las limitantes son los servomotores, los cuales tiene un paso o resolución de 1°, siendo que los cálculos dan una solución en milésimas de ángulo, considerando que estos bloques de servomotores y junto con las cámaras, son únicamente demostrativos, pueden ser aceptables estos valores de los servomotores, puesto que la implementación en el campo real, se harán con motores con resolución a milésimas de grado.

V. Aspectos de seguridad en el sistema

El prototipo actual está implementado con una comunicación alámbrica usando un protocolo serial, esto en el entorno real consideraría el uso de cableado extenso, ya que las distancias reales entre el montaje y el director de tiro son de varios metros, por esa razón, para la siguiente versión del prototipo se podría sustituir por una comunicación inalámbrica. Lo anterior implicaría cambios en la arquitectura propuesta, además de agregar servicios de seguridad como son la autenticación, la confidencialidad y la integridad, los cuales son importantes en un sistema que será usado en un entorno militar. La autenticación es el servicio que trata de asegurar que una comunicación sea auténtica, es decir, verificar que el origen de los datos es el correcto, quién los envío y cuándo fueron enviados y recibidos también sean correctos [9]. Actualmente, la forma de autenticación usando nombre de usuario y contraseña es la más utilizada, por esa razón se debe utilizar un algoritmo de cifrado de contraseñas que sea confiable y seguro. Los algoritmos hash más recomendados actualmente para proteger contraseñas son: Scrypt [3], Bcrypt [10], Argon2 [1], Sha512crypt [6]. Estos algoritmos serán analizados y se seleccionará el que presente mayor ventaja para el sistema propuesto. La confidencialidad es la capacidad de garantizar que la información almacenada en el sistema informático o transmitida por la red. Solamente va a estar disponible para aquellas personas autorizadas a acceder a ella. Si los contenidos son obtenidos por personas ajenas se busca que éstos no puedan acceder a la información o a su interpretación [9]. La integridad busca mantener los datos libres de modificaciones no autorizadas. En otras palabras, la integridad se orienta a mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados [9]. Para establecer un canal seguro en una comunicación inalámbrica, se puede hacer uso de algoritmos de cifrado simétrico, de esta forma se puede conseguir confidencialidad e integridad sin perder velocidad de transferencia de datos. Los algoritmos de cifrado más importantes y que serán analizados para ser incluidos en el prototipo son: Data Encryption Standard (DES) [4], Triple DES (3DES) [7], Advanced Encryption Standard (AES) [5].

VI. Conclusiones y trabajo futuro

En este trabajo, no se logra eliminar la corrección para ángulos menores a 1 grado, pero como se expresó con anterioridad, las limitantes de los equipos que se están usando para implementación y validación de los cálculos, no nos lo permiten, sin embargo, los cálculos, dan solución a problemáticas en milésimas de grados, haciendo con esto un algoritmo muy funcional.

Con esta aplicación y en conjunto con los cálculos de triangulación, este proyecto es totalmente escalable a versiones futuras en la cuales se les podría incluir mejoras, para adquisición de valores y control de varios cañones que se encuentra en barcos más grandes, agregar la adquisición de valores para correcciones de ángulos y distancias desde otro sensores del barco, como lo son radares, GPS, giroscópicas entre otros, también agregar un módulo de designación de objetivos por procesamiento de imágen para la detección de los mismos y varios más. Como trabajo futuro se propone implementar

funciones hash y algoritmos criptográficos para mejorar la seguridad de la plataforma de software en el sistema.

REFERENCIAS

[1] Biryukov, A., Dinu D., Khovratovich D. "Argon2: the memory-hard function for password hashing and other applications", University of Luxemburgo, March 2017.

[2] Cock, J. D. "El método de la triangulación aplicado en un escaner láser, para objetos tridimensionales", Revista Universidad EAFT, 654, pp 25-31, Diciembre 2000.

[3] Colin Percival. "Stronger Key Derivation Via Sequential Memory-Hard Functions".

[4] Han, S.-J., Oh, H.-S., and Park, J. "The improved data encryption standard (des) algorithm. In Spread Spectrum Techniques and Applications Proceedings", 1996., IEEE 4th International Symposium on (Sep 1996), vol. 3, pp. 1310-1314 vol. 3.

[5] Jamil, T. "The rijndael algorithm", IEEE Potentials 23, 2. April 2004.

[6] Movable Type Scripts. "Sha-512 Cryptographic Hash Algorithm", Sitio web: https://www.movable-type.co.uk/scripts/sha512.html, Agosto 2018.

[7] Nadeem, A., and Javed, M. Y. "A performance comparasion of data encryption algorithms", In 2005 International Conference on Information and Communication Technologies, pp 84-89. Aug. 2005.

[8] Reglerteknik S. "Aligner 224 Optical Tracking Evaluation System", de Schill Reglerteknik Sitio web: https://www.schill.se/aligner-224, Marzo 2018.

[9] Stallings, W. "Cryptography and Network Security: Principles and Practice", 5th ed. Pretince Hall Press, Upper Saddle River, NJ, USA, 2010.

[10] Stufft, Donald. "bcrypt: Modern password hashing for your software and your servers", PyPl.

[11] Taylor. G. & Kleeman. L. "Fundations of Visual Perception and Control. At Visual Perception and Robotic Manipulation", pp 16-71, Germany: Springer.

[12] Universidad Politécnica de Madrid. "Métodos Topográficos", de OpenCourseWare Sitio web: http://ocw.upm.es/expresion-grafica-en-la-ingenieria/dibujo-de-construccion/contenidos/MetodosTopograficos/dc3-metodos-topograficos.pdf, Marzo 2018.

Detección de armas en imágenes usando YOLO

Alejandro G. Reyes-Aldeco, Kelsey A. Ramírez-Gutiérrez, Ignacio Algredo-Badillo
Coordinación de Ciencias en Tecnologías de Seguridad
Instituto Nacional de Astrofísica, Óptica y Electrónica
Luis Enrique Erro 1, Sta María Tonanzintla, 72840 San Andrés Cholula, Puebla, México
agreyesaldeco@gmail.com, kramirez@inaoep.mx, algredobadillo@inaoep.mx

***Resumen*—El número creciente de delitos cometidos en los Estados Unidos Mexicanos tienen como principal herramienta el uso de armas de fuego. Varias soluciones tecnológicas se han implementado en los centros de monitoreo dentro del país, donde las soluciones basadas en visión artificial son una de las más importantes. La detección automática de armas puede garantizar la prevención de delitos. En este artículo se presenta un sistema basado en la red neuronal YOLO V3 con el objetivo de detectar armas en un conjunto de imágenes de asaltos, prácticas de tiro y documentales. Adicionalmente, se genera un conjunto de imágenes, las cuales son etiquetadas para que el sistema sea entrenado, probado y validado. Los resultados establecen una opción para que sea implementado en sistemas de videovigilancia ya que se tiene un 84.46 % de exactitud.**

***Index Terms*—CNN, YOLO, Gun-detection**

I. Introducción

Actualmente, en México, el 44.2 % de actividades ilícitas son cometidas con armas de fuego [1]. El crimen y las actividades ilícitas pueden ser reducidas al monitorear e identificar el comportamiento, vestimenta, gestos, entre otros, que comúnmente tienen los delincuentes. Adicionalmente, la percepción de las personas sobre la inseguridad ha ido en aumento en comparación con los años anteriores. Una posible solución a los problemas anteriormente descritos seria desplegar sistemas de control de vigilancia en vehículos y/o edificios con detección de personas armadas además de una alerta a las autoridades.

Los diversos estados de la república mexicana han implementado Centros de Comando y Control, donde se capta información integral para la toma de decisiones en materia de seguridad pública, urgencias médicas, medio ambiente, protección civil, movilidad y servicios a la comunidad a través del vídeo monitoreo, de la captación de llamadas telefónicas y de aplicaciones informáticas de inteligencia, enfocadas a mejorar la calidad de los habitantes. Entre estos se tienen a los C2Móvil (Centros de Comando y Control Móviles) que son vehículos con cámaras desplegables que permiten el monitoreo en lugares de difícil acceso y el envío de imágenes en todo momento a un centro de comando central, y los C4 (Centros de Comando, control, comunicación y computo), C5 (Centros de Comando, Control, Cómputo, Comunicaciones y Contacto Ciudadano) y C5i (Centro de Comando, Control, Cómputo, Comunicaciones, Coordinación e inteligencia) donde se realiza el video monitoreo con la finalidad de prevenir y alertar inmediatamente a las autoridades de seguridad y de emergencias sobre cualquier situación de riesgo.

Los Centros de Comando y control proporcionan imágenes en tiempo real, sin embargo, tan sólo en la ciudad de México han sido instaladas más de 15 mil cámaras de vigilancia, por lo cual resulta complicado anticiparse a los delitos antes de que sucedan debido a la exigencia visual y se necesita una gran número de operadores para observar la totalidad de cámaras.

Con estas fuentes de datos y con ayuda de tecnología es importante tener operaciones basadas en visión artificial (VA) para proporcionar seguridad. En este caso, la VA es un campo de la inteligencia artificial (IA) donde un conjunto de algoritmos son destinados para el procesamiento de imágenes. *Machine Learning* o aprendizaje automático, como parte de la IA, usa algoritmos para extraer información de datos sin procesar, reconocer patrones y representarla en algún tipo de modelo. El *Deep learning* o aprendizaje profundo, forma parte del *machine learning*, cuya meta es llegar a un aprendizaje profundo más avanzado. Entre los algoritmos más populares en el uso del *Deep learning* se encuentran las redes neuronales convolucionales (CNN o ConvNet), que son redes neuronales que son capaces de construir funciones completas a partir de otras menos complejas como puede ser el de reconocimiento de patrones.

Entre las diversas aplicaciones de las redes neuronales, se ha encontrado que ayudan en la detección de patrones, sin embargo, debido a la gran cantidad de algoritmos e implementaciones de redes neuronales convolucionales, no existe una metodología que explique cuál es la mejor red o cuál es el número idóneo de capas que debe contener para realizar una efectiva detección de objetos. Para realizar este tipo de tareas, se necesita un conjunto de datos muy grande, además de realizar numerosas operaciones por lo que el uso de recursos computacionales es muy alto ya que requiere de abundante tiempo para procesarlos y obtener resultados.

La investigación de detección de armas se ha centrado principalmente en la detección de armas y cuchillos, donde se pueden usar sensores costosos y especializados. En la detección de armas, se destacan los sistemas utilizados en el equipaje, basado un escáner de rayos X, como en [2], presenta un método basado en una segmentación robusta [3] y vectores de característicos basados en bordes para la detección automática de potenciales armas en el escaneo de equipaje.

De manera similar, los autores en [4] detectan armas basadas en características de forma en imágenes de rayos X de alta energía, este método tiene una exactitud del 98 %, dando una tasa de alarma más baja y reduciendo el tiempo de inspección

de equipaje.

Los autores en [5] presentan un algoritmo de detección de armas basado en la fusión de imágenes. Las imágenes se obtienen utilizando diferentes sensores y se descomponen en bandas de baja y alta frecuencia con la transformada compleja de doble árbol de doble densidad de Wavelet (DDDTCWT).

Verma [6] implementó un método visual de detección de armas en imágenes usando SIFT (Scale Invariant Feature Transform), el detector de puntos de interés de Harris y Fast Retina Keypoint (FREAK). Alcanzado una precisión de 84.26 %.

Por otro lado, un método híbrido que utiliza segmentación basada en color y un detector de puntos de interés SURF (Speed Up Robust Features), con 88.67 % de precisión alcanzada fue propuesto en [7].

Los trabajos mencionados anteriormente se centran únicamente en la búsqueda de armas por separado (no tienen interacción con personas), sin embargo, [8] ha realizado una implementación de detección de armas utilizando MatConvNet [9] y alcanza una precisión del 93 %. En este sentido, el trabajo propuesto en este artículo se centra en hallar armas aumque otros objetos como personas se encuentren en la escena.

Este artículo se centra en la detección de armas en vídeos en tiempo real por lo que se entrenó una red que analiza vídeo a una velocidad mínima de 15 frames por segundo. El artículo se divide de la siguiente manera: Sección II presenta los antecedentes del trabajo, Sección III detalla el sistema propuesto, Sección IV reporta los resultados y comparaciones y Sección V enuncia las conclusiones y el trabajo a futuro.

II. Fundamentos teóricos

A continuación se presentan los elementos teóricos principales utilizados en el sistema propuesto.

II-A. Redes Neuronales para la detección de objetos

Una tendencia en la detección de objetos en imágenes son las redes neuronales profundas. Además, varios modelos basados en redes neuronales son compartidos públicamente tales como tales GoogLeNet [10], ResNet [11] y YOLO [12] y que se pueden utilizar como inicialización para tareas de entrenamiento, detección y clasificación de objetos.

Las redes neuronales convolucionales han permitido una mejora significativa en el rendimiento de los detectores de objetos, como las Redes neuronales convolucionales basadas en regiones (R-CNNs) [13], que solucionan el problema de la localización con un paradigma basado en regiones.

Un inconveniente de las R-CNN [13] es que toman mucho tiempo de entrenamiento ya que tiene que clasificar demasiadas regiones propuestas por imagen, por lo que está actividad es compleja para ser implementada en tareas de tiempo real y el algoritmo de búsqueda selectiva es un algoritmo fijo. Para mejorar estos problemas, el autor de R-CNN [13] propuso un nuevo algoritmo llamado Fast R-CNN [14], que en vez de alimentar a la CNN con regiones propuestas, se alimenta la CNN con la imagen de entrada para generar un mapa de características convolucionales.

Estos algoritmos usan búsqueda selectiva para encontrar las regiones propuestas. Esta búsqueda es lenta y consume tiempo de procesamiento afectando el desempeño de la red, por lo tanto, Faster R-CNN [15] viene con un algoritmo de detección de objetos que elimina el algoritmo de búsqueda selectiva y deja a la red aprender las regiones propuestas.

YOLO [12] es una arquitectura que proporciona un nuevo enfoque en la detección de objetos, desarrollada en la universidad de Washington, la cual se basa en redes neuronales convolucionales simultáneas que predice múltiples cajas delimitadoras. La red neuronal base trabaja a 45 frames por segundo, esto significa que al procesar video en tiempo real obtiene menos de 25 milisegundos de latencia [16],

A diferencia de los algoritmos basados en regiones mencionados anteriormente, YOLO toma la detección de objetos como un problema único de regresión, en vez de examinar toda la imagen, examina partes de la imagen que tiene altas probabilidades de tener un objeto. Divide la imagen en una cuadrícula de SxS y si el centro de un objeto se encuentra dentro de un cuadrante, ese cuadrante es el responsable de detectar ese objeto. Una sola red convolucional predice simultáneamente múltiples cajas delimitadoras que enmarcan los objetos de la imagen y realiza un mapa de probabilidades por cada clase como lo muestra la fig. 1.

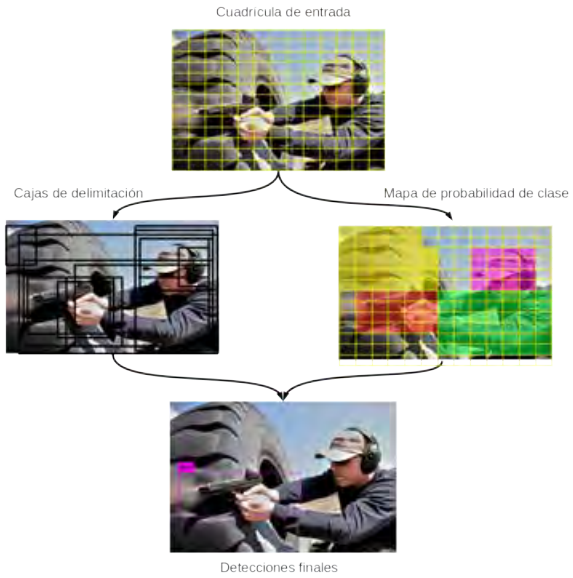


Figura 1: Esquema generar para YOLO.

Su arquitectura se inspiró en el modelo GoogLeNet [10] para la clasificación de imágenes. La red de YOLO tiene 53 capas convolucionales que son llamadas Darknet-53 [17], donde cada capa es idénticamente entrenada con los mismos valores y probadas en cuadriculas de 256 x 256. Se desempeña a la par de clasificadores de vanguardia, pero realiza menos operaciones de punto flotante, lo cual la hace más rápida [17].

III. Diseño y desarrollo del sistema

En este trabajo se propone un sistema para detectar armas de fuego o revólveres basado en las características de YOLO para detectar objetos.

III-A. Selección de imágenes

Consideramos dos conjuntos de imágenes (positivas y negativas), el primer conjunto de imágenes positivas, ver Figuras 2 (a)-(c), son aquellas en las que se presenta el objeto y el segundo conjunto de imágenes negativas, ver Figuras 2 (d)-(f), son aquellas en las que hay ausencia del objeto a identificar y se seleccionaron principalmente donde aparecían personas sosteniendo un objeto. Se seleccionaron un total de 600 imágenes y se dividieron como se muestra en el Cuadro I.

Cuadro I: Distribución de imágenes usadas en este trabajo

Tipo	Positivas	Negativas	Total
Entrenamiento	150	150	300
Pruebas	50	50	100
Validación	100	100	200

III-B. Recolección de imágenes

Las imágenes se obtuvieron de las siguientes fuentes:

III-B1. Internet Movie Firearms Database (IMFDb) [18]: Es una base de datos de imágenes de armas de fuego que aparecen en películas, series de televisión, videojuegos y series animadas. Aunque la base de datos contiene una gran cantidad de armas, este proyecto se centró únicamente en la detección de armas pequeñas como revólveres y pistolas.

III-C. Procesamiento de imágenes

Para cada una de las 300 imágenes utilizadas en el entrenamiento, se debe extraer las posiciones de los objetos, enmarcándolos dentro de un cuadrante interno en la imagen, que se representa mediante coordenadas en píxeles, realizando los siguientes pasos:

1. Seleccionar las imágenes de entrenamiento.
2. Realizar el etiquetado manual de cada imagen, usando la herramienta YOLO MARK [19].
3. Guardar las coordenadas del objeto en una archivo de texto, el archivo se deberá llamar igual que la imagen.

III-D. Entrenamiento

Con el entrenamiento se busca reducir la pérdida de precisión en la detección de objetos, requirió 2000 ciclos de entrenamiento y se utilizó una computadora con 8 GB de RAM, una tarjeta NVIDIA GeForce GTX 1050 TI, un procesador Intel Core I7, CUDA 10.1 y YOLO V3, a través de Darknet-53 [20].

El sistema propuesto basado en YOLO permite detectar, de manera concurrente, armas localizados en diferentes puntos de la imagen que está siendo procesada. Esto es debido a la característica de la red que cada caja delimitadora permite un análisis para definir si hay un arma en ella, es decir, se pueden detectar hasta 5 objetos (armas), una por cada una de las cajas delimitadoras.

IV. Validación y resultados

Las pruebas se realizaron con 100 muestras de imágenes (50 positivas y 50 negativas) diferentes de las utilizadas en el entrenamiento.

Para llevar a cabo la validación del sistema, de 100 imágenes positivas donde se encontraban 106 objetos se detectaron correctamente 95 objetos; por otra parte de 100 imágenes negativas se detectaron erróneamente 21 objetos. Se consideran los siguientes tipos de errores para la evaluación:

1. Error de tipo I. La predicción es positiva cuando el valor debe ser negativo, siendo 21 las ocurrencias de este tipo.
2. Error de tipo 2. La predicción es negativa cuando el valor debe ser positivo, siendo 11 las ocurrencias de este tipo.

Se seleccionaron las siguientes métricas de calidad [21]: *Exactitud (Ac)*, es la proporción del número total de predicciones que fueron correctas. *Tasa de verdaderos positivos (TPR)*, la proporción de que un caso positivo fueran correctamente identificadas. *Tasa de falsos positivos (FPR)*, es la proporción de que un caso negativo haya sido clasificado como positivo incorrectamente. *Tasa de verdadero negativos (TNR)*, la proporción de que los casos negativos fueron correctamente identificados. *Tasa de falsos negativos(FNR)*, la proporción de casos positivos que fueron incorrectamente clasificados como negativos. *Precisión (P)*, la proporción de casos positivos predichos que fueron correctos. El Cuadro II muestra los resultados obtenidos.

Cuadro II: Resultados de las métricas de calidad.

Ac	TPR	FPR	TNR	FNR	P
84.4660	0.89622	0.21	0.79	0.10377	0.818965

En el proceso de evaluación, se obtuvieron los siguientes resultados: *Verdadero positivo*, cuando el objeto es correctamente reconocido como lo muestra la Figura 3, sin embargo, es necesario implementar un supresor para encontrar los valores máximos y así evitar que un objeto sea reconocido más de dos veces. *Falso-Negativo*, cuando el objeto no es reconocido satisfactoriamente, como se muestra en la Figura 4 y *Falso-Positivo* cuando se identifican objetos incorrectos como correctos, como se puede ver en la Figura 5.

V. Conclusiones

De acuerdo a los resultados cuando se entrena el detector YOLO en varios escenarios y condiciones es robusto, respecto a las imágenes el tiempo de detección es de 47,5 milisegundos en promedio.

En la Figura 6 se muestra la comparación de exactitud de este trabajo con otros similares. En [6] y [7], donde no se aplica entrenamiento, utilizan segmentación basada en colores y su cantidad de imágenes es menor (88 imágenes para el primer caso y 25 imágenes para el segundo), este trabajo obtiene una exactitud similar a [6] y 4.2 % menor respecto a [7], sin embargo, el tiempo de detección de ambos es proporcional al numero de objetos que se encuentran en la imagen.

(a) (b) (c)

(d) (e) (f)

Figura 2: Muestra de imágenes

Figura 3: Positivo verdadero.

Figura 4: Falso Negativo.

Figura 5: Falso positivo.

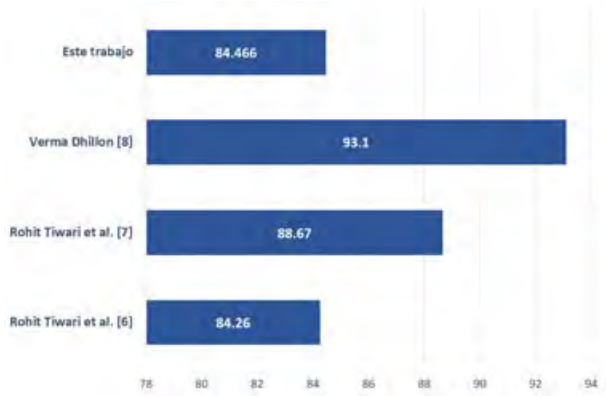


Figura 6: Comparación de la exactitud obtenida con trabajos similares.

La precisión de [8] es mayor en 8.6 % donde se aplica una arquitectura VGG-16 basada en CNN como un extractor de características. Aunque las imágenes positivas son similares, las imágenes negativas de [8] se eligieron de forma aleatoria, mientras que nuestras imágenes se centraron principalmente en personas que tenían diversos objetos en las manos.

Se observó que al entrenar la red neuronal con una muestra pequeña de imágenes ocasionan que frecuentemente se detecten como positivos algunos objetos negativos, por lo que es necesario volver a realizar el entrenamiento con una muestra mas grande de imágenes para mejorar la precisión.

Referencias

[1] INEGI, "Encuesta nacional de victimización y percepción sobre seguridad pública principales resultados(envipe) 2018," 2018.

[2] S. Nercessian, K. Panetta, and S. Agaian, "Automatic detection of potential threat objects in x-ray luggage scan images," 06 2008, pp. 504 – 509.

[3] Maneesha Singh and Sameer Singh, "Image segmentation optimisation for x-ray images of airline luggage," in *Proceedings of the 2004 IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety, 2004. CIHSPS 2004.*, July 2004, pp. 10–17.

[4] A. D. Lopez, E. S. Kollialil, and K. G. Gopan, "Adaptive neuro-fuzzy classifier for weapon detection in x-ray images of luggage using zernike moments and shape context descriptor," in *2013 Third International Conference on Advances in Computing and Communications*, Aug 2013, pp. 46–49.

[5] T. Xu and Q. M. Jonathan Wu, "Multisensor concealed weapon detection using the image fusion approach," in *6th International Conference on Imaging for Crime Prevention and Detection (ICDP-15)*, July 2015, pp. 1–7.

[6] G. Verma and R. Tiwari, "A computer vision based framework for visual gun detection using harris interest point detector," vol. 54, 08 2015.

[7] G. Verma, "A computer vision based framework for visual gun detection using surf," 01 2015.

[8] G. Verma and A. Dhillon, "A handheld gun detection using faster r-cnn deep learning," 11 2017, pp. 84–88.

[9] A. Vedaldi and K. Lenc, "Matconvnet - convolutional neural networks for MATLAB," *CoRR*, vol. abs/1412.4564, 2014. [Online]. Available: http://arxiv.org/abs/1412.4564

[10] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. E. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, and A. Rabinovich, "Going deeper with convolutions," *CoRR*, vol. abs/1409.4842, 2014. [Online]. Available: http://arxiv.org/abs/1409.4842
[11] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," *CoRR*, vol. abs/1512.03385, 2015. [Online]. Available: http://arxiv.org/abs/1512.03385
[12] J. Redmon and A. Farhadi, "YOLO9000: better, faster, stronger," *CoRR*, vol. abs/1612.08242, 2016. [Online]. Available: http://arxiv.org/abs/1612.08242
[13] R. B. Girshick, J. Donahue, T. Darrell, and J. Malik, "Rich feature hierarchies for accurate object detection and semantic segmentation," *CoRR*, vol. abs/1311.2524, 2013. [Online]. Available: http://arxiv.org/abs/1311.2524
[14] R. Girshick, "Fast rcnn," *IEEE International Conference onComputer Vision (ICCV)*, 2015.
[15] S. Ren, K. He, R. Girshick, and J. Sun, "Faster r-cnn: Towards real-time object detection with region proposal networks," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 39, no. 6, pp. 1137–1149, June 2017.
[16] J. Redmon, S. K. Divvala, R. B. Girshick, and A. Farhadi, "You only look once: Unified, real-time object detection," *CoRR*, vol. abs/1506.02640, 2015. [Online]. Available: http://arxiv.org/abs/1506.02640
[17] J. Redmon and A. Farhadi, "Yolov3: An incremental improvement," *CoRR*, vol. abs/1804.02767, 2018. [Online]. Available: http://arxiv.org/abs/1804.02767
[18] (2019) Internet movie firearms database imfdb. [Online]. Available: http://www.imfdb.org/wiki/Main_Page
[19] AlexeyAB, "Yolo mark," 2019. [Online]. Available: https://github.com/AlexeyAB/Yolo_mark
[20] ——, "Darknet-53," 2019. [Online]. Available: https://github.com/AlexeyAB/darknet
[21] EcuRed, "Matrices de confusión," 2019. [Online]. Available:

Panorama de la Normatividad Internacional respecto a la Privacidad de los Datos de los Usuarios de Internet

Víctor Reyes-Macedo, Gina Gallegos-García, Moisés Salinas-Rosales
Instituto Politécnico Nacional - Centro de Investigación en Computación
Av. Juan de Dios Bátiz sn casi esq. Miguel Othón de Mendizábal
Unidad Profesional Adolfo López Mateos Col. Nueva Industrial Vallejo
Alcaldía Gustavo A. Madero C.P 07738, Ciudad de México, México
vreyesm1102@alumno.ipn.mx , ggallegosg@ipn.mx, msalinasr@ipn.mx

***Resumen*—Este trabajo provee al lector de un panorama general sobre la normatividad internacional de la privacidad en el contexto de la cuarta revolución industrial, la era de las comunicaciones y la información. Lo anterior cobra relevancia en un contexto social internacional en donde han surgido controversias respecto a la privacidad de los datos de los usuarios. Para ello, se abordarán tres enfoques: tratados internacionales, legislaciones locales y legislación mexicana. Destaca el hecho de que existen pocos instrumentos legales que permitan a los usuarios de Internet garantizar su derecho a la privacidad, debido a que el contexto de las comunicaciones por este medio recién empieza a ser tomada en cuenta para elaborar dichos instrumentos. De hecho, sólo la Unión Europea y el estado de California en Estados Unidos de América cuentan con un documento que considera específicamente este caso. Los demás, son adaptaciones e interpretaciones de instrumentos de protección de datos ya existentes, como en el caso de México.**

***Index Terms*—Anonimato, derechos humanos, legislación, privacidad , tratados internacionales**

I. Introducción

En el actual contexto global, las tecnologías de la información y comunicación han permitido conectar las diferentes regiones del mundo, haciendo posible el intercambio de información de manera instántanea prácticamente en cualquier lugar. Lo anterior ha generado la apertura de nuevos campos de actividad económica y social para las personas. Por ejemplo, la información generada por los usuarios de plataformas tecnológicas que proveen diferentes servicios, es analizada y usada por las empresas para incrementar sus ganancias mediante diferentes estrategias mercadológicas. Para ello, los usuarios aceptan términos y condiciones de uso que en ocasiones atentan contra su privacidad. De esta forma, otorgan poder a los proveedores de servicios para usar la información generada, con fines comerciales, políticos, y de investigación, entre otros.

Debido a la importancia de la información personal que con diversos motivos se brinda a las empresas u organizaciones a través de Internet, es importante el desarrollo de marcos legales que protejan a los usuarios contra un potencial uso indebido de su información. Por ello, la contribución de este artículo se centra en brindar un panorama sobre la legislación alrededor de este tema en el mundo.

El lector encontrará el artículo organizado de la siguiente forma: en la sección II se habla de conceptos básicos del tema, la sección III aborda los tratados internacionales que retoman la privacidad como un derecho de las personas, la sección IV describe las características de las principales legislaciones en materia de protección de datos que se han desarrollado a nivel regional o nacional. Posteriormente, la sección V retomará el caso de México, y se finaliza con la sección VI que aborda los principales retos y oportunidades para avanzar en este tema.

II. Conceptos Iniciales

En un sentido general, es posible entender el concepto de *privacidad* como la acción de mantener en secreto el contexto en el cual se desarrolla una actividad, a diferencia del *anonimato*, que se centra en mantener secreta la identidad de quien desarrolla una actividad. Por ejemplo, la información bancaria de un tercero es información privada, ya que los datos de los movimientos que realiza no son de acceso público, aún si todos saben a quién pertenece dicha cuenta [1].

El derecho a la privacidad y a la protección de datos es uno de los temas prioritarios en el debate internacional, impulsado en parte por la cantidad de servicios que recolectan y comercian con ellos. A través del tiempo, se han propuesto diversos marcos legales con diferentes objetivos y alcances para proteger los datos de los usuarios de Internet. Sin embargo, no existe un único instrumento legal para abordar problemas sobre seguridad en el ciberespacio, sino que las posibles soluciones surgen de la colaboración entre diferentes disciplinas.

Debido a lo anterior, existen diferentes instrumentos que pueden ser aplicados al entorno digital, como los que se enumeran a continuación. Cabe destacar que a nivel interno, la constitución nacional prevalece sobre otros instrumentos [2].

1. **Tratado:** Se trata de un convenio regido por el derecho internacional público, celebrado por escrito entre Estados o entre Estados y otros sujetos de derecho

internacional, como organizaciones, y bajo el cual cada una de las partes asumen compromisos [3].

2. **Políticas públicas nacionales:** Es una intervención deliberada del Estado, para corregir o modificar una situación reconocida como problema público. También se denomina política pública a las decisiones transversales que regulan la actuación interna de los gobiernos y que están destinadas a perfeccionar la gestión pública [3].
3. **Marcos jurídicos:** Conjunto de disposiciones, leyes, reglamentos y acuerdos a los que debe apegarse una dependencia o entidad en el ejercicio de las funciones que tienen encomendadas [3].
4. **Códigos de buenas prácticas:** Fórmulas que han demostrado, por medio de la investigación y la evaluación, su eficacia y sostenibilidad, que producen resultados sobresalientes y que pueden ser aplicables y adaptables a otras situaciones [4].

III. Normatividad Internacional

Un tratado internacional es un acuerdo celebrado por escrito entre Estados, o entre Estados y otros sujetos de derecho internacional, como las organizaciones internacionales, y regido por el derecho internacional [5]. En este nivel, el documento que aborda el tema de la protección de datos y la privacidad, es la *Declaración Universal de Derechos Humanos*, a través de la resolución *A/HRC/20/L.13 Promoción, Protección y Disfrute de los Derechos Humanos en Internet*, la cual declara que los derechos humanos deben estar garantizados en el mundo digital de la misma forma que en el mundo físico.

Varios acuerdos internacionales reconocen el derecho a la privacidad. Por ejemplo, la *Declaración Universal de Derechos Humanos*, establece en su 12° artículo: "Nadie será sometido a interferencia arbitraria con su privacidad, familia, hogar o correspondencia, ni a ataques contra su honor y reputación. Toda persona tiene derecho a la protección de la ley contra tales interferencias o ataques [6]"

Por otra parte, la Asamblea General de las Naciones Unidas, a través del documento A/C.3/71/L.39 *El derecho a la privacidad en la era digital* [7] reconoce que un entorno abierto, seguro, estable, accesible y pacífico en el ciberespacio es sumamente importante para la realización del derecho a la privacidad en la era digital. Luego, reafirma el derecho a la privacidad establecido en el artículo 12 de la *Declaración Universal de Derechos Humanos*, y el artículo 17 del *Pacto Internacional de Derechos Civiles y Políticos*. Reconoce, además, la naturaleza abierta de internet y el rápido avance de las tecnologías de la información, y por ello afirma que los derechos de las personas también deben estar protegidos en internet, incluyendo el derecho a la privacidad. Exhorta a los estados a que respeten y protejan el derecho a la privacidad en el contexto de las comunicaciones digitales, y que adopten las medidas para poner fin a las violaciones de esos derechos. Adicionalmente deben cerciorarse de que sus leyes se ajusten a sus obligaciones en virtud del derecho internacional, y a que examinen sus procedimientos, prácticas y legislaciones relativos a la vigilancia y la intercepción de las comunicaciones y la recopilación de datos personales.

Según el derecho internacional, los estados deben respetar la privacidad de las personas, mientras se aseguran de que terceros no participen en comportamientos que puedan afectar arbitrariamente su privacidad, la obligación se extiende al contexto de las comunicaciones digitales y la recopilación de datos personales [2].

En la misma dirección, el artículo 11 del *Pacto Internacional de Derechos Civiles y Políticos* retoma el texto mencionado anteriormente y agrega que "toda persona tiene derecho a la protección de la ley contra tales interferencias o ataques [8]".

IV. Normatividad Regional

Además de los tratados internacionales, el debate sobre el derecho a la privacidad ha llevado a diversos países a generar legislaciones locales que protejan a los usuarios en este tema. Entre estas destacan el *convenio número 108 del Consejo de Europa* [9], la *Directiva 2002/58/CE del Parlamento Europeo y del Consejo* [10] y el *Reglamento General de Protección de Datos (RGPD)* [11] en Europa, así como la *Ley de Transferibilidad y Responsabilidad del Seguro Sanitario (HIPAA)* [12], la *Ley Federal de Transacciones Crediticias Justas y Exactas (FATCA)* [13] y el *Acta de Privacidad del Consumidor de California* [14]. Finalmente, se presenta la *Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP)* [15] correspondiente a la legislación mexicana.

Los instrumentos mencionados se describen a continuación.

IV-A. Unión Europea

Uno de los primeros antecedentes en Europa es el *convenio número 108 del Consejo de Europa,* del 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, el cual destaca por ser el primer instrumento internacional legalmente vinculante adoptado en el ámbito de la protección de datos [9].

Además, en 2002 se aprobó la *Directiva 2002/58/CE del Parlamento Europeo y del Consejo*, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (directiva sobre la privacidad y las comunicaciones electrónicas) [10], que entre sus consideraciones, define *la esfera privada de los usuarios, que debe ser protegida*, de la siguiente manera:

"Los equipos terminales de los usuarios de redes de comunicaciones electrónicas, así como toda información almacenada en dichos equipos, forman parte de la esfera privada de los usuarios que debe ser protegida de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Los denominados «programas espía» (spyware), web bugs, identificadores ocultos y otros dispositivos similares pueden introducirse en el terminal del usuario sin su conocimiento para acceder a información, archivar información oculta o rastrear las actividades del usuario, lo que puede suponer una grave intrusión en la intimidad de dichos usuarios. Sólo debe permitirse la utilización de tales

dispositivos con fines legítimos y con el conocimiento de los usuarios afectados."

Por otro lado, la Unión Europea aprobó el 14 de abril del 2016 el *Reglamento General de Protección de Datos (RGPD)*, cuyos objetivos incluyen [11]:

- Armonizar las leyes de privacidad de datos en toda Europa.
- Proteger y potenciar la privacidad de los datos de todos los ciudadanos de la UE.
- Cambiar la forma en que las organizaciones de toda la región abordan la privacidad de los datos.

El RGPD incluye, en su artículo 78, la siguiente declaración:

"La protección de los derechos y libertades de las personas físicas sobre el procesamiento de datos personales requiere que se tomen las medidas técnicas y organizativas apropiadas para garantizar que se cumplan los requisitos del presente Reglamento. Para poder demostrar el cumplimiento de este Reglamento, el controlador debe adoptar políticas internas e implementar medidas que cumplan en particular los principios de protección de datos por diseño y protección de datos por defecto. Dichas medidas podrían consistir, entre otras cosas, en minimizar el procesamiento de datos personales, pseudonimizar los datos personales lo antes posible, la transparencia en relación con las funciones y el procesamiento de los datos personales, permitir que el interesado monitoree el procesamiento de los datos, permitiendo que el controlador cree y mejorar las características de seguridad ... "

IV-B. Estados Unidos

A diferencia de Europa, las leyes de los Estados Unidos de América son reconocidas por ser más laxas en cuanto a protección de datos, y en general protegen la información personal de sus ciudadanos del acceso exterior.

Una de estas leyes es la *Ley de Transferibilidad y Responsabilidad del Seguro Sanitario (HIPAA)* [12]. Esta ley federal crea protecciones para información relacionada con la salud individual. Específicamente, quién puede tener acceso a la información relativa a la salud de sus ciudadanos.

Por otro lado, la *Ley Federal de Transacciones Crediticias Justas y Exactas (FATCA)* [13], está diseñada para ayudar a proteger la información de crédito de los consumidores de los riesgos asociados con el robo de datos, no obstante su intención es prevenir que los contribuyentes estadounidenses utilicen cuentas financieras fuera de los EE.UU. con el fin de evadir impuestos.

Finalmente, el estado de California aprobó en 2018, el *Acta de Privacidad del Consumidor de California*, la cual se convirtió en la legislación más estricta en materia de protección de datos en el país. En ella, el usuario adquiere el derecho de pedir a una empresa que no comparta ni venda su información personal. Además, obtiene el control sobre la información personal que recopila una empresa y las responsabiliza de salvaguardar su información personal [14].

IV-C. Organización para la Cooperación de Desarrollo Económico

El 23 de septiembre de 1980, los países miembros de la OCDE acordaron las *Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales* [16]. Si bien el documento puede ser considerado como antiguo, ha servido como una de las guías para sentar las bases de la protección de datos personales en medios digitales. Mediante el documento mencionado, recomienda "que los países miembros tengan en cuenta en su legislación interna los principios relativos a la protección de la privacidad y las libertades individuales". Además, deben esforzarse por eliminar o evitar que aparezcan,en nombre de la protección de la privacidad, obstáculos injustificados para los flujos transfronterizos de datos personales. En esencia, este documento requiere que la información cumpla con los siguientes puntos.

- Obtención legal y justa.
- Uso sólo para el propósito originalmente especificado.
- Ser adecuada, relevante y no excesiva a su propósito.
- Correcta y actualizada.
- Accesible al sujeto.
- Almacenada de manera segura.
- Destruida una vez que haya cumplido su propósito.

V. Normatividad Mexicana

En México, el instrumento existente es la *Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP)* [15], promulgada el 5 de julio de 2010. La LFPDPPP, define dato personal como cualquier información concerniente a una persona física identificada o identificable, y prevé una definicion de *dato sensible*, para aquello referente a datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.

Este documento, establece en su artículo 1º, lo siguiente:

"La presente Ley de orden público y de observancia general en toda la República y tiene por objeto la protección de los datos personales en posesión de los particulares, con la determinación de regular su tratamiento legítimo, controlado e informado, un efecto de proteger la privacidad y el derecho a la autodeterminación informativa de las personas ".

Además, se establecen los principios de protección de datos personales, las autoridades reguladoras y las sanciones aplicables en caso de no cumplirse con las disposiciones establecidas. Y aunque reconoce a los datos personales como un *insumo de la economía digital*, no establece directrices específicas para el entorno de las tecnologías de la información.

El artículo 112 del reglamento de la LFPDPPP considera el tratamiento automático de la información, e invoca la obligación del responsable del almacenamiento de datos de informar al titular el tratamiento de los mismo, lo cual es aplicable en sistemas automatizados de tratamiento de datos. Sin embargo, el texto carece de fuerza ante la recolección de datos que hacen en Internet las empresas privadas con establecimientos en otros países. De esta forma, de frente al

desarrollo de nuevas tecnologías y maneras de procesar, analizar, almacenar y utilizar los datos personales, el reglamento se vuelve obsoleto.

VI. Conclusiones

Como se ha visto, la privacidad ha sido abordada en varios instrumentos legales con el objetivo de garantizar la protección de los datos de los usuarios, y con ello su seguridad. Sin embargo, uno de los principales retos es la dificultad de aplicar estas leyes al contexto digital, bien por interpretación o bien por jurisdicción. Por otro lado, es claro que se necesitan leyes acorde al contexto tecnológico, como el RGPD en la Unión Europea o el Acta de Privacidad del Consumidor de California, que consideren los aspectos relacionados con el diseño de infraestructura, hardware, código, y demás aplicables a los servicios que recaban datos y comercian con ellos. Además, se debe considerar el hecho de que los proveedores de los servicios no se ubican siempre en el lugar geográfico dónde la legislación tiene validez, por lo que deben diseñarse los instrumentos legales necesarios para proteger a los usuarios. Por otro lado, en el caso de México, el único instrumento que aborda el tratamiento de información personal es la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares.* Sin embargo, no contempla de manera específica el caso de la información en Internet, los datos recabados por empresas asentadas en el extranjero ni las nuevas formas de procesar y almacenar información de este tipo. Por ello, es importante desarrollar una estrategia integral, alineada a los tratados internacionales de derechos humanos y civiles, que permita establecer un marco normativo que asegure a los usuarios el respeto a su privacidad, considerando el avance de las tecnologías de comunicaciones.

Agradecimientos

Los autores agradecen al Instituto Politécnico Nacional, que a través del Centro de Investigación en Computación, brindó el apoyo necesario para la realización de esta investigación, a través de los proyectos con número SIP 1917 y SIP 20196694.

Referencias

[1] D. Bradbury, "Anonymity and privacy: a guide for the perplexed," *Network Security*, vol. 2014, no. 10, pp. 10–14, 2014.
[2] A. Becerril, "Industria 4.0 vs leyes 0.9," INFOTEC, Octubre 2018.
[3] O. Montoya, "Diccionario jurídico." [Online]. Available: http://www.diccionariojuridico.mx/
[4] T. Ausín, "Buenas prácticas (códigos de)= best practices (codes of)," *EUNOMÍA. Revista en Cultura de la Legalidad*, no. 15, pp. 239–248, 2018.
[5] U. E. y. C. Ministerio de Asuntos Exteriores. Tratados internacionales. [Online]. Available: http://bit.do/e7Rw8
[6] U. G. Assembly, "Universal declaration of human rights," *UN General Assembly*, vol. 302, no. 2, 1948.
[7] "El derecho a la privacidad en la era digital." [Online]. Available: https://acnur.org/fileadmin/Documentos/BDL/2017/10904.pdf
[8] International covenant on civil and political rights. [Online]. Available: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx
[9] C. de Europa, "Convenio n° 108 del consejo de europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal," 1981.
[10] U. Europea, "Directiva 2006/24/ce del parlamento europeo y del consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la directiva 2002/58/ce, diario oficial de la unión europea," *DO L*, vol. 105, no. 13.04, 2006.
[11] Directive 95/46/ec (general data protection regulation). [Online]. Available: https://eugdpr.org
[12] H. C. Assistance, "Summary of the hipaa privacy rule," *Office for Civil Rights*, 2003.
[13] IRS. Foreign account tax compliance act (fatca). [Online]. Available: https://www.irs.gov/businesses/corporations/foreign-account-tax-compliance-act-fatca
[14] "Home: California consumer privacy act." [Online]. Available: https://www.caprivacy.org/
[15] C. de Diputados, "Ley federal de protección de datos personales en posesión de los particulares," *Diario Oficial de la Federación, Distrito Federal*, 2010.
[16] O. for Economic Co-operation and Development, *OECD guidelines on the protection of privacy and transborder flows of personal data*. OECD Publishing, 2002.

Sistema de información automotriz basado en un esquema de seguridad y protección jurídica

Diana Carolina Carrión Martínez, *Estudiante Maestría, INAOE,* Alejandro Medina Santiago, *Investigador, INAOE,* Ignacio Algredo Badillo, *Investigador, INAOE*

***Abstract*—En México los accidentes automovilísticos con daños materiales y/o humanos requieren realizar una investigación pericial ya que es obligatoría por ley, con el objetivo de descubrir lo sucedido y las causas del mismo. Sin embargo, existen ocasiones donde las pruebas son insuficientes para comprender lo sucedido o bien éstas han sido alteradas. El presente trabajo propone un dispositivo electrónico utilizando un sistema embebido basado en microcontroladores, eligiendolo por su capacidad de programación empleando un lenguaje de alto nivel, para realizar una tarea específica así como obtener una mayor eficiencia de sus componentes; guarda los datos generados por los sensores que se encuentran integrados dentro de los automóviles. Se agrega un esquema de seguridad para evitar que los datos sean alterados por algún elemento externo antes, durante o después de que el accidente automovilístico se produzca. El esquema propuesto ocupa blockchain, funciones hash, cifrado AES aunado a un esquema jurídico; el primero y segundo para asegurar la integridad durante todo el proceso jurídico mientras que el tercero para dar privacidad a los datos mientras son transferidos del automóvil a la máquina donde se examinan. Asimismo se propone un protocolo jurídico, planteando el manejo de las llaves de descifrado para o dentro del sistema jurídico mexicano disponiendo del mismo para tal propósito; en el manejo correcto de evidencias de los datos generados por el automóvil, empleados o usados para evidencia válida en caso de accidente automovilístico.**

***Index Terms*—Sistemas embebidos, AES, Funciones Hash, Protocolo Jurídico, Esquema de Seguridad, IoT**

I. Introducción

En el año 2017 en México se registraron un total de 367,789 accidentes automovilísticos solo considerando zonas urbanas y suburbanas [1]; cuando en éstos existen consecuencias con daños, tanto materiales como humanos, citando al capítulo VI artículo 183 del reglamento de Tránsito en Carreteras Federales [2], se realizará una investigación de los hechos por parte de la autoridad correspondiente. Sin embargo existen panoramas donde el automóvil queda dañado a un nivel que hace difícil el comprender lo que realmente ocurrió en la escena y/o los hechos en ella son ambiguos, dificultando el aclarar los hechos. De igual manera hay otro problema, la manipulación de la escena del crimen, incluyendo los indicios que se encuentran en esta, ya sea de forma natural, interviniendo elementos como la lluvia, animales y demás; o de forma artificial, siendo manipulado por alguna persona con la intención de obtener algún beneficio, afectando la declaración final del investigador y el veredicto que se dará.

La era tecnológica en la cual se encuentra la sociedad ha permitido el usar la ciencia en casi cualquier sitio para resolver problemas y automatizar procesos gracias a la gran aceptación que esta ha tenido, se persigue de forma constante el mejorar y hacer las tareas de forma más eficaz, produciendo tecnologías cada vez más eficientes, rápidas, fáciles de usar, atractivas, visionarias, etc. Para obtener una mayor cantidad de beneficios se requiere tener un mejor control sobre el intercambio de información que se da entre los sistemas, por lo que existe la intención de que cada vez más dispositivos se encuentren conectados a la red, generando e intercambiando de forma constante datos. Esto representa un gran desafío tanto de logística como de seguridad, puesto que dichos dispositivos contienen información privada, si los mismos que la crean y distribuyen no poseen un sistema de seguridad apropiado, el robo de información es probable .

Actualmente existen diferentes formas de proteger la información que se encuentra en formato digital, el tipo de protección que se dará dependerá de la necesidad que se tenga o lo que se desee hacer con la información; un ejemplo de método de protección para la información es el de un algoritmo que la modifica de un formato legible a un formato codificado, con el fín de que sea difícil el comprender y de esta forma darle confidencialidad al mensaje, cuando se desee regresar el mensaje a su estado original es necesario poseer una "llave" o clave que es usada junto con operaciones matemáticas para la alteración del texto de un formato legible a ilegible y viceversa. Estas operaciones se llaman algoritmos de cifrado y se enfocan en el área que el autor requiera, como ejemplo el asegurar la protección de la información con un algoritmo más robusto y complejo sacrificando el tiempo ejecución así como los recursos a usar.

Otros procedimientos que sirven para la protección de la información son las marcas de agua digitales, se emplean para ocultar información dentro de un objeto digital, introduciendo una cadena de bits en el mensaje que se enviará sin que afecte de forma visible o detectable al objeto, ocupando este método se busca que el mensaje pase desapercibido. El tipo de algoritmo utilizado para comprobar la integridad de los datos son las funciones hash, cuando un mensaje es introducido se hace uso de un algoritmo, el cual transforma dicho mensaje en una cadena de bits incomprensible que, a diferencia de los algoritmos anteriormente mencionados, la cadena de caracteres, resultado de la operación matemática realizada tendrá siempre la misma longitud. Si el contenido del mensaje cambia en lo más mínimo el resultado de la transformación cambia de igual manera de forma que resulte sencillo el notar la alteración en el mensaje. La función hash se creó con la particularidad de que una vez alterados los datos estos no volverán a formar el mensaje original, a lo anterior se

le conoce como picar y mezclar; gracias a las características de este algoritmo se usa para la autenticación de los datos, al comparar la cadena de datos que resulta de la operación, a la cual se le conoce como digesto, antes de realizar alguna acción en la cual el mensaje se pudo haber modificado con la generada despues de dicho acontecimiento.

La necesidad de proteger la información existe para todos los dispositivos que la generan puesto que el no hacerlo puede llegar a perjudicar los mismos. Una de las áreas a las cuales no se le ha puesto la suficiente atención a la protección de los datos es en el sector automotriz donde, para mejorar el control y modernizar sus productos las empresas automotrices agregan sensores, los cuales ayudan al conductor a tener una mejor experiencia, así como un sistema más intuitivo; mientras que del lado del software apoya mejorando la conducción. Contribuyendo a generar una gran cantidad de datos, que podrían servir para mejorar la experiencia de los usuarios de los automóviles o para realizar acciones malintencionadas.

Anteriormente se han creado sistemas como [3], [4] y [5] que ayudan a esclarecer los accidentes automovilísticos, estos han llegado a ser desde simples cámaras de video hasta sistemas avanzados que ayudan a determinar la situación del vehículo, llevando un seguimiento de lo que sucede alrededor haciendo uso de los distintos dispositivos con los que cuenta. En otros países ya se ha implementado sistemas de caja negra en los automóviles al darse cuenta de la creciente necesidad de dicho dispositivo ayudando en la investigación, asimismo proporcionando información sobre lo sucedido durante el accidente. Aunque existe el debate sobre si estos objetos violan los derechos de privacidad de los individuos a consecuencia de que los investigadores pueden descargar los datos contenidos en la caja negra sin necesidad de autorización previa del dueño, siendo que las leyes que deberían regular esto no son claras al respecto, aumentando la polémica con respecto a este aspecto; en la siguiente sección se describirá la situación jurídica actual con respecto al tratamiento de datos informáticos.

Se describira, en la sección III, el sistema propuesto buscando ayudar en la investigación de accidentes relacionados con vehículos, así como proporcionar una herramienta que apoye los procesos de averiguación. Proponiendo un sistema sencillo, útil y que cuente con la información necesaria para lograr tal tarea de forma satisfactoria. El sistema contendrá datos en forma de texto plano, obtenidos a partir de los sensores ya existentes dentro del automóvil, lo cual evitará el tener que agregar dispositivos y/o sistemas extras. Los datos al ser obtenidos por los sensores del mismo automóvil aportará conocimiento sobre su funcionamiento interno y si existieron problemas en este antes o durante el accidente.

II. Situación Jurídica

El 17 de Junio del año 2016 se llegó a un acuerdo general por parte de la Consejo de la Judicatura Federal, por el que se expide el Protocolo de actuación para la obtención y tratamiento de los recursos informáticos y/o evidencias digitales. Donde se manifiestan los deberes y compromisos que el poder judicial tiene para con los nuevos recursos tecnológicos y la protección que se debe dar por parte del poder judicial. Se consideran las obligaciones ya presentes en la constitución, las cuales son: la normatividad y los criterios para modernizar los sistemas y procedimientos administrativos internos, conformidad con el artículo 81, fracción XVIII, de la Ley Orgánica del Poder Judicial de la Federación; con el auge de las tecnologías de la información, es necesario proporcionar métodos y procedimientos que aseguren la detección, recolección, manejo, autentificación, análisis, procesamiento y resguardo de los recursos informáticos y/o evidencias digitales. La obtención de la información (elementos de prueba) constituye una de las facetas útiles dentro del éxito de una investigación, aspecto que demanda de los encargados de la recolección, preservación, análisis y presentación de las evidencias, una eficaz labor que garantice la autenticidad e integridad de estas, a fin de ser utilizadas posteriormente como parte de los diversos procedimientos que se tramitan en el Consejo de la Judicatura Federal y/o en su caso, ante las autoridades ministeriales o judiciales correspondientes, entre otras. Por lo anterior se acuerda un protocolo de actuación para la obtención y tratamiento de los recursos informáticos y/o evidencias digitales el cual toca los tópicos de: *I. Procedencia, II. Inspección, detección, aseguramiento y documentación, III. Recolección, IV. Registro, V. Embalaje, VI. Traslado y entrega para análisis, VII. Desembalaje, VIII. Análisis e informes, IX. Almacenamiento en el lugar de resguardo, X. Traslado para la presentación de los recursos informáticos y/o evidencia digital como Material probatorio, XI. Destino final.*

III. Sistema propuesto

El objetivo de este trabajo es presentar un protocolo jurídico, implementar un esquema de seguridad y desarrollar un dispositivo electrónico. El primero utiliza artículos y acuerdos para dar relevancia a los datos digitales obtenidos a través del dispositivo electrónico, y que sean considerados como evidencia probatoria sin que su ambiente sea un inconveniente para ello. El esquema de seguridad sirve para dar confidencialidad a los datos, así como para certificarlos durante todo el proceso como auténticos e íntegros, en caso contrario existe una forma de comprobar que tal alteración se ha llevado a cabo, esto al comparar las cadenas picadillos creadas a partir de la función hash y blockchain con los datos almacenados; por último, el dispositivo electrónico se ocupa de recopilar, guardar, procesar y enviar la información obtenida de los sensores del automóviles al dispositivo donde el investigador custodiará los datos.

Se expondrán los elementos que intervienen:

- Peritos, expertos en determinada materia, proporcionan información confiable y objetiva, producto de la aplicación del método científico y de técnicas especializadas; [6]
- Investigador, alguien que lleva adelante un proyecto orientado a la búsqueda de conocimiento y al esclarecimiento de hechos y de relaciones; [7]
- Evidencia, prueba determinante; [8]
- Juez de control, Órgano Jurisdiccional del Distrito Federal que interviene desde el principio del procedimiento y hasta el dictado del auto de apertura a juicio; [9]

- Llave de descifrado, porción de información que es utilizada para convertir un mensaje legible a una forma ilegible y viceversa; [10]
- Automóvil, vehículo autopropulsado destinado al transporte de personas o mercancías sin necesidad de carriles; [11]
- Bases de datos, conjunto de datos pertenecientes a un mismo contexto y almacenados; [12]
- Dispositivo, pieza o conjunto de piezas o elementos preparados para realizar una función determinada; [13]
- Sensores, aquello que tiene una propiedad sensible a una magnitud del medio, y al variar esta magnitud también varía con cierta intensidad la propiedad; [14]
- Repositorio, espacio centralizado donde se almacena, organiza, mantiene y difunde información digital; [15]
- Sistema embebido, sistema de computación diseñado para realizar una o algunas pocas funciones dedicadas. [16]

A. Metodología Jurídico

La metodología que se siguió para la parte jurídica, actuando los peritos, la evidencia digital, el juez de control y la llave de descifrado; en la cual se siguen los siguientes pasos durante su realización: a) revisar las leyes actuales concernientes a las evidencias digitales, b) examinar los procedimientos en caso de accidentes automovilísticos, c) analizar los sensores que proporcionan datos relevantes para la investigación y d) proponer una metodología jurídica que dé relevancia a la evidencia digital. Se revisan las leyes actuales que atañen a las evidencias digitales, así como el tratamiento que estas reciben desde la escena del crimen hasta su disposición, tales como [17], [18], [19], el artículo 251 del código nacional de procedimientos penales, donde se indica que es necesaria la autorización de un juez de control para descifrar la información que se encuentre dentro del dispositivo electrónico [20] y el artículo 9 de la Ley Modelo sobre el Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional [21], donde se estipula que toda información presentada en forma de mensaje de datos gozará de la debida fuerza probatoria. De igual forma se revisa cómo se tratan las evidencias y el procedimiento legal que se gestiona en caso de un accidente automovilístico con daños materiales y/o humanos, el cual se encuentra estipulado en el Manual para el manejo de la evidencia digital así como en Lineamientos para la obtención y tratamiento de los recursos informáticos y/o evidencias digitales, el último estipulado por el Poder Judicial de la Federación Consejo de la Judicatura Federal [22].

A continuación se hace una investigación, para conocer los sensores que se encuentran dentro del automóvil y proporcionan datos relevantes que ayudan a aclarar los hechos ocurridos antes, durante y después del accidente, así como las condiciones en las cuales se encontraba el automóvil, para esto se consulta a un perito judicial automotriz, así como a un experto automotriz. Una vez realizadas las correspondientes entrevistas se indaga sobre los sensores más comunes que se encuentran en las distintas marcas de automóviles. Se explica más acerca de los sensores en la sección de dispositivo electrónico.

La propuesta metodológica jurídica, apoya en dar relevancia a los datos aportados por los sensores, proporcionando les una base legal que los considere como un indicio fiable así como una pieza clave para el comprender los hechos ocurridos que afectaron al automóvil y/o que resultaron en el accidente automovilístico; para lograr esto se hace uso de las leyes existentes y procedimientos establecidos para la manipulación de la evidencia digital cuando existe la necesidad de una investigación o se ha pedido una por cualquiera de las partes involucradas.

La metodología indica que las empresas automotrices creen las llaves y las guarden; en caso de que exista un accidente de tráfico y las respectivas sean requeridas por el juez de control necesitara una orden judicial donde solicitará la llave antes mencionada a la empresa correspondiente y en cuanto ingrese dentro de la investigación será tratada como evidencia, por lo que tendrá su propia cadena de custodia teniendo, de esta forma, que seguir los lineamientos que se marcan para evitar su extravío o que se cree una copia no autorizada de la misma.

Cumplido la llave su objetivo, el cual es el descifrado de los datos, se buscará su pronta eliminación siguiendo los protocolos establecidos para lograr tal propósito; así como los procedimientos adecuados establecidos para tal finalidad. Se tendrá un programa que se emplea tanto para el descifrado de los datos como para la verificación de los mismos ocupando blockchain, funciones hash y el descifrador AES, dicho programa no guarda las llaves ni las claves se ocupan para realizar las tareas anteriores esto con la finalidad de evitar cualquier filtración de información importante que pueda llegar a afectar casos parecidos.

Las llaves se dejan al cuidado de las empresas y decidiendo estás como guardar las mismas, aunque se espera que se almacenen en una sola sede central y en ellas se salvaguarden dichas llaves, evitando que la información se filtre o extravíe. Se llevará un mejor control de las llaves y la información durante la investigación judicial gracias a que las primeras entran en la cadena de custodia desde que son entregadas al juez de control por lo que se tiene una estricta vigilancia sobre ellas desde que entran en la carpeta de investigación hasta que las mismas son desechadas.

Con respecto a la asignación de las llaves a los automóviles, las empresas decidirán cómo y de qué forma. La metodología jurídica antes descrita se representa en la figura **??**.

B. Esquema de Seguridad

En esta parte se consideran los actores que vienen siendo el automóvil, los peritos, los investigadores, las bases de datos, el dispositivo y los sensores.

Asimismo existen los procesos de almacenamiento seguro y recepción. En el *proceso de almacenamiento seguro* los datos son extraídos de los sensores dentro del automóvil y almacenados por el dispositivo electrónico. A partir de aquí el sistema: a) genera una cadena de caracteres única ocupando blockchain, b) cifra los datos ocupando AES y c) produce una cadena de caracteres única a toda la base de datos ocupando SHA-2. En el *proceso de recepción* los datos enviados del dispositivo electrónico dentro del automóvil se

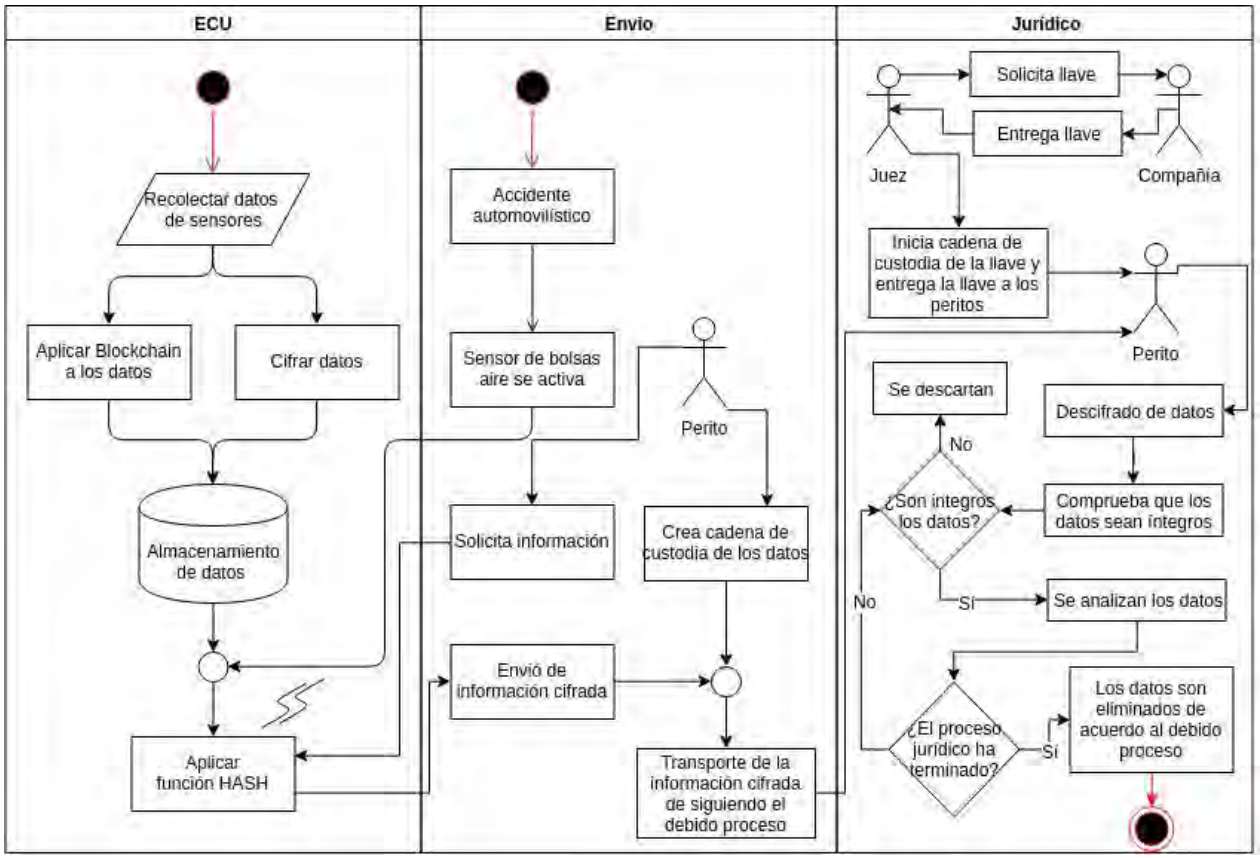


Fig. 1: Diagrama de flujo del sistema propuesto

reciben y almacenan dentro de un dispositivo digital en el cual el perito o investigador observa los datos obtenidos. En esta parte se: a) comprueba que la base de datos no ha sido alterada comparando la cadena de caracteres que procede desde la extracción, con la que se genera en el sistema del perito: b) descifra la información utilizando la llave obtenida del proceso jurídico y: c) comprueba la autenticidad de los datos comprobando la última cadena de caracteres de cada base de datos con la cadena generada por el sistema del investigador ocupando la llave obtenida por el proceso jurídico.

Se va a detallar el proceso de almacenamiento seguro a continuación:

En la parte de seguridad se busca que los datos extraídos de los sensores se ocupen para ayudar a esclarecer los hechos ocurridos en un accidente, sean confiables y ante cualquier intento de manipulación, exista una forma de advertir así como de comprobar que tales alteraciones se han realizado. Para esto, lo primero que se realizó fue encontrar una forma comprobar que los datos no han sido alterados durante el proceso de investigación, por lo tal es necesario tener una forma de comprobar que la modificación no ha ocurrido o que estos se hayan corrompido, puesto que si existe una mínima modificación de los mismos pueden ser descartados como evidencia al haber sesgo en la información; a continuación se necesita proteger los datos, evitando el que se puedan comprender el contenido que se encuentra guardado en el dispositivo electrónico otorgandole confidencialidad; posteriormente se perseguirá la integridad de la base de datos complera, esto con el propósito de, si existe alteración alguna, por cualquier medio o circunstancia se corrobore la misma.

La integridad de los datos es importante, ya que con la misma se puede comprobar que durante todo el proceso los datos han sido los mismos, haciéndolos legítimos. Para lograr dicho se ha elegido el blockchain [23] puesto que es un registro único, consensuado y distribuido en varios bloques, y gracias a que cada bloque contiene una cadena de caracteres particular conseguido después de ejecutar el blockchain, es factible el comprobar la integridad de los datos de forma sencilla, donde el proceso opera detectando si los datos han sido modificados, al agregar una cadena de caracteres al final de cada línea. El blockchain funciona de la siguiente manera: las cadenas de caracteres anteriormente mencionadas se cuentan de igual manera y al llegar a los 128 bits se extrae la función picadillo de las mismas, para esto se necesitan lo siguiente: la función picadillo anterior, la cadena anteriormente mencionada, una clave y la fecha junto con la hora en que se realizó dicha acción. Esto se repite hasta que todos los bloques de 128 bits cuentan con su cadena de caracteres resultante de la función picadillo. Una vez realizado la comprobación de la integridad se continua con la protección.

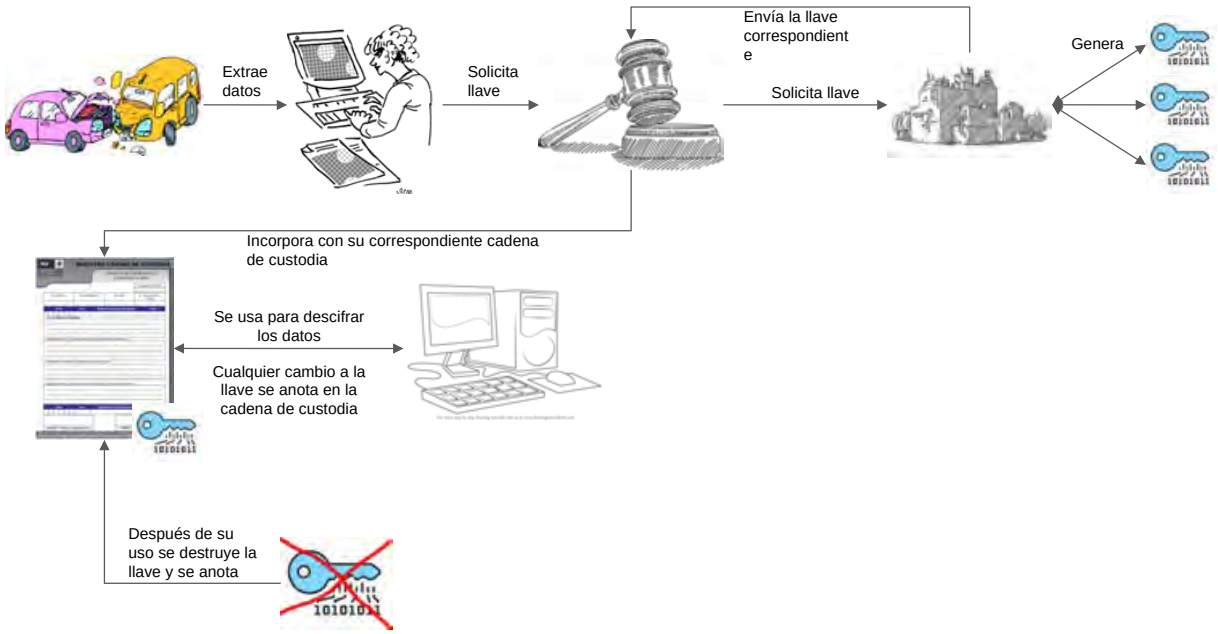


Fig. 2: Diagrama de flujo del protocolo jurídico

Para la confidencialidad de los datos se resolvió el cifrarlos, ya que dicho método transforma las cadenas de caracteres en un texto incomprensible así como el mensaje creado dificulta el que se pueda adivinar o, por medio de fuerza bruta, descifrar el texto original a menos que se tenga la llave de descifrado. Existen distintos tipos de cifrados, entre los cuales se encuentran los asimétricos y simétricos; se decidió ocupar el tipo de cifrado simétrico por la rapidez y simplicidad al momento de realizar los cálculos en comparación con el cifrado asimétrico. Una vez seleccionado el tipo de cifrado a usar se investigó entre los existentes decidiendo por el AES esto debido a que actualmente se encuentra entre los más seguros, conocidos y utilizados, al cual hasta el momento en que se escribe este artículo, los ataques a este cifrado no han tenido éxito y solo existen propuestas de ataque que podrían llegar a vulnerarlo aprovechando el sistema matemático ordenado en el que se basa.

El cifrado AES [24] funciona dentro del dispositivo de la siguiente manera, se cuentan los datos de los sensores que entran, cuando estos alcanzan el tamaño de requerido en bits comienza el cifrado de los datos haciendo uso de rondas donde en cada una de estas, un byte es reemplazado por otro. Los bits de ciertas columnas son rotadas de manera cíclica con otros bits de otras columnas para luego ser mezcladas y por último cada byte es combinado con la clave del round, esto se hace un determinado número de veces, definido por el tamaño de los bloques, lo que finalmente nos el mensaje cifrado.

Posteriormente estos datos se convierten en un archivo, a dicho archivo se le genera su código hash. El hash previo de la cadena anterior se guarda en un archivo en conjunto con el de los bloques de datos; ayudando a agregar otra capa de seguridad, la cual sirve para verificar que el archivo general no se modificó durante el traslado de un dispositivo a otro, puesto que el hash que se genera después de cifrar los datos y antes de enviarlos, lo que permite que al dispositivo recibirlos este pueda hacer el digesto del archivo y corroborar que estos no estén alterados por cualquier razón. La función hash elegida para realizar dicha tarea es el SHA-2 [25], puesto que, aunque actualmente ya existe el SHA-3, el SHA-2 todavía sigue vigente y hasta el momento no existen ataques que puedan dañar la seguridad del digesto.

Ahora se detallará el proceso de recepción; una vez obtenidos los datos, se comprueba que éstos sean auténticos al comparar la cadena hash incluida en el archivo con la generada por el sistema del perito utilizando la base de datos adquirida; seguidamente se descifrara dicha con la llave de descifrado, obtenida a través del proceso jurídico antes mencionado y el descifrador del AES. Una vez los datos se encuentren en forma de texto plano comprensible será posible comprobar si estos han sido modificados desde que salieron del dispositivo gracias a la cadena de caracteres del valor hash que se le incrustó a cada línea de datos con la generada por el sistema utilizando la clave obtenida. Puede comprobar que estos son integros al checar la última cadena hash creada, puesto que si ésta varía significa que los datos, ya sea por algún elemento externo o por corrupción, han sido alterados. En la figura 3 se observa el diagrama de flujo del Esquema de Seguridad que ya se ha explicado, en la figura 4 se detalla mas profundamente el proceso de almacenamiento seguro, mientras que en la figura 5 es el proceso de recepción lo que se expone.

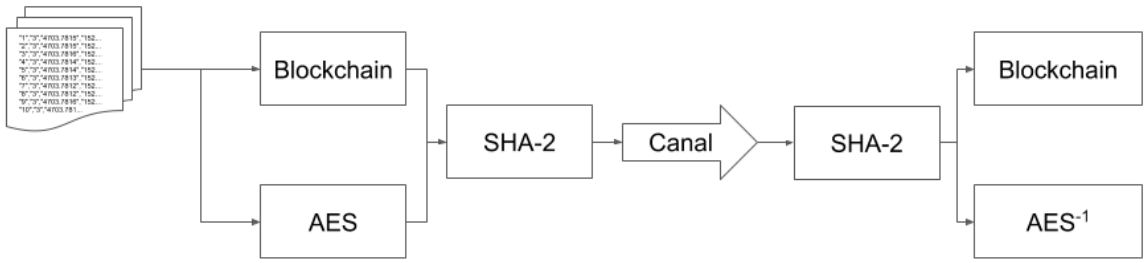


Fig. 3: Diagrama de flujo del Esquema de Seguridad

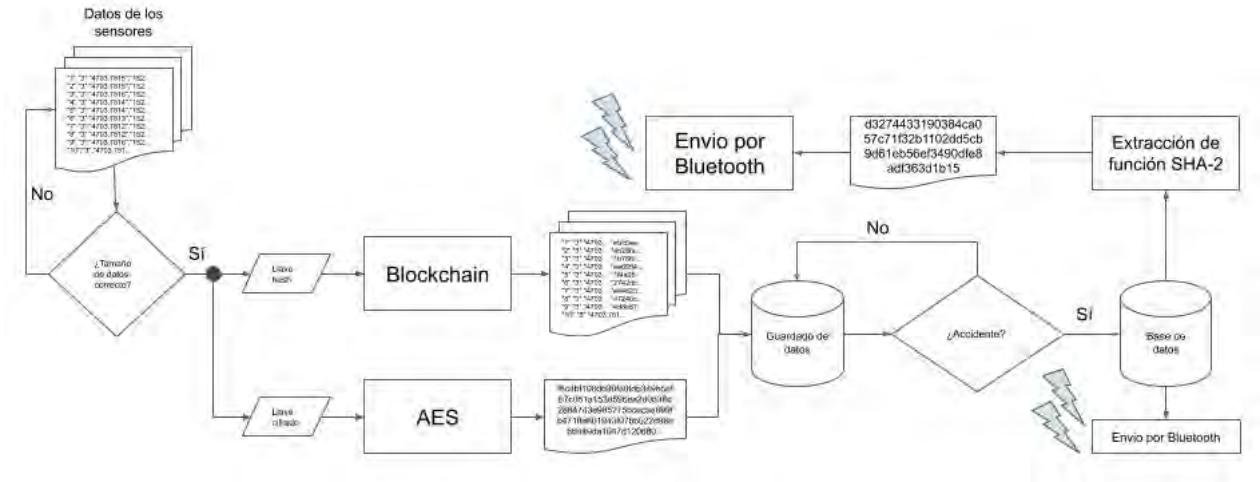


Fig. 4: Diagrama de flujo del proceso de almacenamiento seguro

C. Dispositivo electrónico

Los actores considerados para esta sección son el dispositivo electrónico, el repositorio, el automóvil, los sistemas embebidos y los sensores. En tanto los pasos a seguir son: a) examinar y escoger los sensores, b) extraer los datos de los sensores y crear un repositorio con estos, c) analizar la información de los sensores, d) analizar las necesidades para con los datos y su tratamiento, e) seleccionar los dispositivos a usar y f) armar el dispositivo.

Se procede a examinar los sensores que contiene el automóvil con la finalidad de ubicar aquellos que podrían servir en una investigación judicial o para las aseguradoras. Con el objetivo de lograr esto, se entrevistó a peritos vehiculares así como a expertos en el área automotriz con la meta de conocer los sensores que tomarían más relevancia en caso de accidente y de estos, cuáles son los más comunes que se encuentran en los automóviles; ya elegidos los sensores se extraen los datos y se crea un repositorio con el propósito de tener una gran cantidad de información para realizar experimentos y comprobar resultados. Entre los sensores elegidos para crear dicho repositorio están considerados los sensores de seguridad, algunos de los cuales son los siguientes: Radar telemétrico (el cual sirve para la prevención de colisión), sensor de ocupación de asiento (cuando hay un choque, éste indica dónde se activan las bolsas de aire), sensor de inclinación de ruedas (indica la posición en la que se encuentran las ruedas), sensor de inclinación (ayuda a la regulación de los faros), sensor de aceleración (detectan la aceleración en curvas así como para activar sistemas de protección de los pasajeros), sensor de vuelco (se activa cuando un ángulo varía respecto su posición de montaje), sensor de velocidad de giro de las ruedas (ABS), entre otros.

También se consideraron otros sensores como el sensor de posición del pedal, esto para saber qué tanto el conductor estaba apretando el acelerador o el freno o si en todo caso los estaba apretando; el sensor de presión de aceite y combustible, sensor de presión del líquido de freno, y demás. El repositorio sirve para analizar los datos, realizar los algoritmos que aseguran la información, así como tener al alcance diferentes datos de diferentes sensores de diferentes modelos de automóviles, lo cual ayuda a tener mayor rango para confirmar el correcto funcionamiento del software y hardware.

Con los datos extraídos que los sensores generan, analizando y comprendiendo la misma se descifra como los sensores representan, en texto plano, la información que les corresponde registrar, por ejemplo el sensor de posición nos da los sigu-

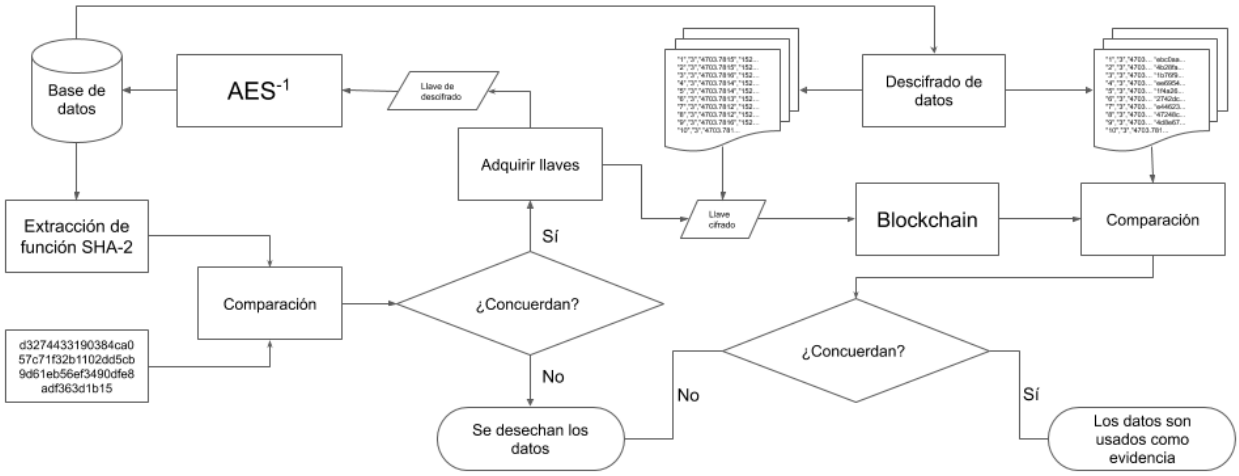


Fig. 5: Diagrama de flujo del proceso de recepción

ientes datos: ”1”,”3”,”4703.7815”,”1527.4713”,”359.9”,”2017-01-19 16:19:04.742113”, donde el primer dato es el id de posición; el segundo es el id del viaje; el tercero es la latitud; el cuarto la longitud; el quinto la altitud y el último la fecha y hora.

Se advierte de la necesidad de almacenar los datos dentro del dispositivo electrónico, así como procesarlos usando un esquema de seguridad, el cual ya se ha mencionado anteriormente, con la finalidad de protegerlos de algún daño a nivel software o si existe alguno identificar tal, y enviarlos de un dispositivo a otro usando algún medio de transmisión; de igual manera se busca que éste sea económico, tenga la suficiente memoria para almacenar el código necesario para realizar las funciones anteriormente nombradas, así como para almacenar los datos extraídos de los sensores del automóvil y una velocidad de procesamiento aceptable tomando en consideración el uso que se la va a dar. Con todo lo anteriormente mencionado, se desarrolla el dispositivo electrónico deseado.

Para logralo, sin recurrir a placas armadas, se analizó las opciones existentes en el mercado y las características con las que cada una cuenta, considerando como prioridad la velocidad del procesamiento de los datos con las que estas cuentan, lo que terminó con la elección de un sistema embebido, puesto que dispone de las entradas necesarias para soportar los módulos que se ocuparan, así como la capacidad de memoria necesaria para almacenar el código que se implementa y la velocidad de procesamiento con la cuenta es aceptable para lo que se pretenden realizar. En la tabla I se hará una comparación del ATmega2560 contra el sistema embebido Nano, la cual fue considerada como una placa a ocupar, explicando el porque de que el ATmega2560 fuera elegido.

Como se puede observar el voltaje que utilizan ambas es el mismo, pero mientras el número de pines en el ATmega2560 es mayor son los necesarios para conectar los módulos que se ocupan. La velocidad de reloj es la misma en ambos sistemas embebidos, sin embargo la Memoria Flash y la SRAM son mayores en el ATmega2560 ayudando a la velocidad de procesamiento de los datos; siendo éstas las principales razones para dicha elección.

	ATmega2560	Nano
Voltaje	5V	5V
Pines	54 D, 16 A	14 D, 8 A
Memoria Flash	256 KB	16 KB
SRAM	8 KB	1 KB
EEPROM	4 KB	512 bytes
Clock Speed	16 MHz	16 MHz

TABLE I: Comparación de las características de los arduinos ATmega2560 y Nano

Para la parte del envío de datos de un dispositivo a otro se analizaron las opciones de envío de forma alámbrica e inalámbrica optando por esta última; llegando a esta resolución cuando se vieron los pro y contras de cada una de las opciones. Mientras que la alámbrica podría dar más seguridad, al necesitar de conectarse directamente al dispositivo para sustraer la información, evitando el enviarlos de forma indiscriminada a los dispositivos cercanos como lo hace la comunicación inalámbrica, la misma es una desventaja considerable, puesto que en caso de un accidente catastrófico el conectarse al dispositivo sería casi imposible o, si este se encuentra en lugares de difícil acceso causaría retrasos en la investigación o incluso el no obtener la misma, ya que el conectarse ocupando algún medio físico sería casi imposible, sino hasta que se recupere el dispositivo; por lo cual se decidió que el envío de los datos de forma inalámbrica sería la mejor opción.

Ya resuelto que la forma de envío de datos se realiza por medios inalámbricos se procedió a elegir el tipo a usar. Las opciones que se discutieron fueron Wi-Fi y Bluetooth, quedando la última como la seleccionada por las razones se enlistan a continuación.

- En el caso de Wi-Fi el consumo de energía es elevado comparado con el Bluetooth, lo cual ayuda en dicho trabajo que busca reducir en lo posible dicha características para que se pueda utilizar en otras funciones.

- El rango de envío de datos está limitado a unos 30 m alrededor del dispositivo, en el caso de Bluetooth; dicho tamaño de área es aceptable en caso de necesitar extraer la información de un área poco accesible.

Decidido el método de transmisión a continuación se decide el tipo de módulo que se ocupara para dicha tarea, siendo el Bluetooth BLE SH-HC-08 y como su nombre lo indica es un Bluetooth Low Energy o Bluetooth de baja energía, que contiene el nuevo protocolo v4, dicho está pensando en disminuir todo lo posible la necesidad de energía de los dispositivos que lo usan.

Detallado lo anterior así como los sensores que se van a utilizar, se procede a ocuparse de los datos con la finalidad de prepararlos para la siguiente fase. En la figura 6 se observa el diagrama del sistema embebido, mostrando el dispositivo electrónico finalizado, los módulos que se van a emplear son: el módulo SDCard, el cual almacena la información y el módulo Bluetooth el cual se encarga de enviar la información cuando la misma es requerida. El módulo Bluetooth se encontrara en modo stand-by, es decir, sin enviar una señal como comunicarse con otro dispositivo, si no hasta que el accidente automovilístico ocurra, momento en el que el sistema embebido y la programación dentro de él lo active y el mismo comience a enviar una señal a la espera de una contestación para conectarse al dispositivo que contenga la clave correcta.

IV. Conclusiones

El sistema judicial actual en México se encuentra atrasado con respecto a incorporar a las leyes para las tecnologías de la información así como el asistirse con éstas, lo que genera una carencia a la hora utilizar y juzgar las mismas. Esto provoca que en caso de cometerse un delito donde se encuentren involucrados recursos tecnológicos, se dé un veredicto incorrecto o que el proceso se alargue más de lo necesario, existiendo la posibilidad de probar o ayudar a demostrar la inocencia o culpabilidad de una persona haciendo uso de los recursos obtenidos. Y al no existir una legislación que respalde dicha evidencia durante los procedimientos legales y jurídicos la misma es descartada. Por ello es necesario comprender el cómo funciona la tecnología y los avances que ofrece, de esta forma se dará un uso más efectivo de ella. Se tiene la intención de que el dispositivo propuesto ayude no sólo como evidencia válida durante investigaciones judiciales, sino también como un método de prevención, al comprender lo sucedido, el saber cómo, dónde y por qué ocurrió tal incidente. Se espera que este dispositivo no solo ayude a la justicia mexicana sino también a las personas.

References

[1] INEGI. (2018) Accidentes de tránsito terrestre en zonas urbanas y suburbanas. [Online]. Available: https://www.inegi.org.mx/sistemas/olap/proyectos/bd/continuas/transporte/accidentes.asp

[2] R. de Tránsito en Carreteras y Puentes de Jurisdicción Federal, "Artículo 183," 11 2012.

[3] H. Mansor, K. Markantonakis, R. N. Akram, K. Mayes, and I. Gurulian, "Log your car: The non-invasive vehicle forensics," in *2016 IEEE Trustcom/BigDataSE/ISPA*, Aug 2016, pp. 974–982.

[4] X. Yi, A. Bouguettaya, D. Georgakopoulos, A. Song, and J. Willemson, "Privacy protection for wireless medical sensor data," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 3, pp. 369–380, May 2016.

[5] R. S. S. k. B. A. U. V. C. V. Roja, R. Revathi, "Intelligent safety using smart blackbox," *SSRG International Journal of Electronics and Communication Engineering*, vol. 5, March 2015.

[6] P. R. Guerra, *El Ministerio Publico y su vinculo con los servicios periciales*, 1st ed. "", 11 2017, ch. 14, pp. 2–77.

[7] anonimo, "Investigador," 2019, Última actualización 20 jul 2019 a las 12:56. [Online]. Available: https://es.wikipedia.org/wiki/Investigador

[8] J. Martínez, "Evidencia," 2017, diccionario Social — Enciclopedia Jurídica Online. [Online]. Available: https://diccionario.leyderecho.org/evidencia/

[9] D. G. de Servicios Legales, "Glosario," 2019, gobierno de la Ciudad de México. [Online]. Available: https://data.consejeria.cdmx.gob.mx/index.php/dgsl/glosario/Glosario-Consejera-1/J/JUEZ-DE-CONTROL-31/

[10] G. J. Simmons, "A survey of information authentication," *Proceedings of the IEEE*, vol. 76, no. 5, pp. 603–620, May 1988.

[11] R. A. Española, *Automóvil*, 23rd ed., ser. 15. Felipe IV, 4 - 28014 Madrid: Real Academia Española, 7 2018, vol. 1, edición del Tricentenario.

[12] J. D. Ullman, *A first course in database systems*. Upper Saddle River, N.J: Prentice Hall, 1997.

[13] J. P. P. y María Merino, "DefiniciÓn de dispositivo," 2014. [Online]. Available: https://definicion.de/dispositivo/

[14] S. Bennett and I. of Electrical Engineers, *A History of Control Engineering, 1930-1955*, ser. Control, Robotics and Sensors Series. P. Peregrinus, 1993. [Online]. Available: https://books.google.com.mx/books?id=VD_b81J3yFoC

[15] M. R. Domínguez López, *Los derechos de autor y el uso de los repositorios institucionales en México*. México: UNAM, 5 2014, p. 60, consultado el 23 de enero de 2017.

[16] M. Barr, "Embedded systems glossary," 4 2007.

[17] B. J. BECERRA, "El proceso civil en méxico," *México: Porrúa SA*, 2006.

[18] J. O. Favela, *Derecho procesal civil*. Oxford University Press, 2013.

[19] M. A. D. de Léon, *Las pruebas en el derecho procesal del trabajo*. Textos universitarios, 1981.

[20] C. N. de Procedimientos Penales, "Artículo 251," 7 2014.

[21] L. M. sobre el Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, "Artículo 9," 12 1996.

[22] P. J. D. L. F. C. D. L. J. Federal, *Lineamientos Para La Obtención Y Tratamiento De Los Recursos Informáticos Y/O Evidencias Digitales*. México: Poder Judicial De La Federación Consejo De La Judicatura Federal, 6 2016, p. 11.

[23] L. FORTNEY, "Blockchain explained," 2019, last accessed 21 September 2019. [Online]. Available: https://www.investopedia.com/terms/b/blockchain.asp

[24] U. S. N. I. of Standards and T. (NIST), "Announcing the advanced encryption standard (aes)," 11 2001, federal Information Processing Standards Publication 197.

[25] P. C. v. O. Alfred J. Menezes and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 8 2001, vol. 5.

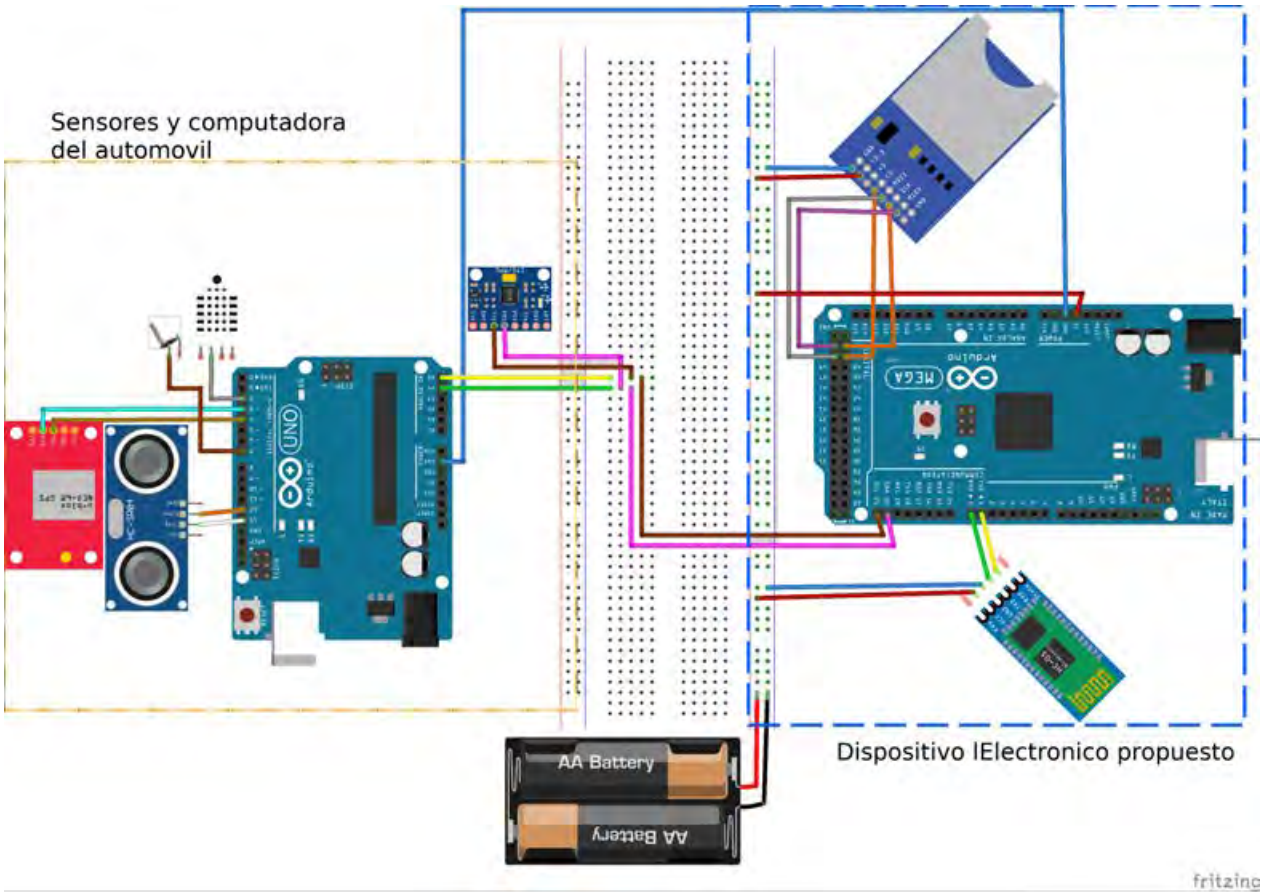


Fig. 6: Diagrama del protoboard del dispositivo electrónico

Control y Monitoreo IoT de una carga Digital/Analógica para Smartphone

Mario Alberto Castillo Rosete
Instituto Nacional de Astrofísica, Óptica y Electrónica
Luis Enrique Erro #1, Sta. Maria Tonantzintla, Puebla, CP 72840,

México
castillo@inaoep.mx

Abstracto—En el presente trabajo, se describe la implementación de un sistema para señalización vía SSH para comunicar por medio de Ethernet y/o WiFi el software App Inventor y el Hardware Arduino Yun ambos desarrollados bajo licencias GPL, para monitoreo y control remoto del encendido y apagado de una carga a 110 volts. Esta comunicación no solamente indica una orden de acción, en este caso de encendido, sino que también informa sobre el estado de la carga, es decir, el usuario sabe si la carga esta activada o desactivada.

A su vez la comunicación entre ambas partes es cifrada con una llave pública y una privada para garantizar que el certificado por medio de SSL y RSA indique que la información transmitida y recibida viaja por un canal seguro de comunicación entre el cliente y el servidor. De acuerdo a los resultados obtenidos el sistema propuesto representa una buena solución en el monitoreo de cargas por medio de dispositivos móviles.

I. INTRODUCCIÓN

La industria 4.0 presenta una serie de retos y oportunidades, donde se muestra que los últimos desarrollos tecnológicos que impulsarán la competitividad industrial ofrecen, más que un producto final, una experiencia de un servicio que conlleve a la resolución de problemas y necesidades actuales dentro de una nube de información y procesos de producción. Así como el análisis de datos que cada día van revolucionando hasta llegar a una rápida reacción de solución a la media de clientes o usuarios, generando la ingeniería social.

II. DESCRIPCIÓN DEL SISTEMA

El proceso es gestionado por un servidor LAM que robustece la autentificación para brindar el servicio web por medio del protocolo HTTPS donde posteriormente se almacena y se analizan la información en una base de datos en MySQL que conforma nuestro servidor virtual.

Fig. 1. Automatización de Procesos

Hoy en día, las empresas tienen el reto de adaptar la producción de acuerdo a la demanda en tiempo real, por lo tanto, se requiere de la colaboración e integración de todos los procesos para poner en el centro de todo al cliente o usuario final. Es aquí donde se habla del cloud computing, fabricación aditiva y fabricación flexible, todo para lograr que los procesos tengan un sentido dentro del internet de las cosas, en donde el usuario sienta la libertad de movimiento y conectividad.

ISSN: 3061-8991

III. ALCANCES DEL SISTEMA PROPUESTO

Crear un modelo de infraestructura que este dentro de los sectores estratégicos de la revolución industrial, en este caso es el de las telecomunicaciones y que el trabajo de control y monitoreo de cargas vía Ethernet o WiFi, aporte soluciones a la red de infraestructura crítica dentro de un ciclo de trabajo, ya sea en el ámbito residencial o industrial.

IV. OBJETIVOS DEL SISTEMA

A) Seguridad

Que el presente trabajo cuente con un modelo de seguridad, que genere confianza y que trate de prevenir incidentes tanto del mundo físico como del mundo lógico, para evitar afectaciones en la infraestructura de los clientes o usuarios y así ofrecer una seguridad en ambientes físicos y lógicos.

B) Desarrollo Tecnológico

Que los beneficios de un ecosistema digital, sean detonadores de tecnologías que impacte en igualdad a los sectores de la población, optimizando los recursos económicos, al estar conectados a internet para ir en paralelo con un desarrollo tecnológico.

C) Digitalización

Digitalizar la información mediante la conexión en internet, creando un modelo dinámico con factores externos que afecte el proceso de control y monitoreo de una carga digital o analógica, llevando un esquema que traslade el concepto de operación, hacia el concepto de inteligencia en la digitalización de estados físicos a lógicos.

Fig. 2. IoT en los procesos de manufactura

V. AUTOMATIZACIÓN, PROCESOS Y FLUJOS DE TRABAJO

El internet de las cosas cada vez es más relevante hoy en día, no solo se trata de conectar cosas cotidianas a internet, también permite la integración y conexión entre las personas, los datos y las máquinas, dando lugar a sistemas de información integrales con operación remota para ser accedidos con la finalidad de transmitir y recibir instrucciones desde servidores externos conectados con el internet, que impactarán directamente sobre la productividad y eficiencia de diversos sectores como la industria, el sector salud, la infraestructura urbana y el medio ambiente.

Fig. 3. El internet de las cosas rumbo a la Industria 4.0

En este trabajo el dispositivo Arduino Yun, se conecta para realizar una tarea de control y monitoreo complejo, en donde se gestionan diversos protocolos de seguridad, los cuales identificarán irregularidades diversas como ataques cibernéticos al servicio de control y monitoreo.

Es por ello que, al implementar una gestión más precisa y eficiente en la transmisión y recepción de datos recabados por los diversos sensores que conforma nuestro sistema, dará una implementación que pasará de ser solo un elemento de control de activación de carga, a ser ahora un elemento que se encargue del monitoreo activo, mediante la lectura de datos provenientes de los sensores que indiquen el estado de la carga, ya sea activa o fuera de línea.

VI. COMUNICACIÓN DEL SISTEMA

La información recopilada de los sensores, adquirirá mayor relevancia y será clave para su análisis y ocupación para la toma de decisiones sobre el estado de la carga. Ya sea para su producción o mantenimiento dentro del ciclo de control y monitoreo.

De esta manera, implementando nuevos y diversos sensores a diferentes cargas sean digitales o analógicas, surgirán nuevas propuestas para la implementación de esta herramienta de control y monitoreo remoto IoT para Smartphone, la cual nos brinda una integración de información total al sistema que gestiona el servidor, el cual maneja una cantidad inmensa de datos provenientes de diversas fuentes de sensores, lo cual representa el control y monitoreo de diferentes cargas que se manejen a 110 volts. Como, por ejemplo, en términos residenciales integrando el encendido y apagado de luminarias, cámaras de seguridad, electrodomésticos, etc. Y en términos industriales el encendido o apagado de cargas como lo es el aire acondicionado de un centro de datos, sistemas de cómputo, entre muchos otros.

VII. DESARROLLO DEL SISTEMA

Dentro de una era digital nos encontramos con los principales talentos que son las PYMES, las cuales en su incansable esfuerzo por establecerse van creando trabajos del futuro para sobrevivir dentro de un mundo globalizado, pero mejor aún para crecer apalancándose de los beneficios digitales.

Por otra parte, la utilización de los nuevos medios y aplicaciones que se utilizan para realizar diversas operaciones, están cambiando en gran medida distintos aspectos de la organización social y económica que se deriva de la gran conectividad que el ser humano interactúe en un ambiente digital de la vida diaria. Por ello, se espera adoptar una transformación, la cual hoy en día ya no es una opción, es una necesidad a diversos retos que resolver a los que se enfrenta cada persona día a día.

VIII. PROBLEMÁTICA

La disponibilidad de la información es vital en la Industria 4.0, la múltiple variedad de tecnologías involucra una alta conectividad en redes LAN, MAN, WAN y VLAN, lo que también expone a infinidad de vulnerabilidades de ambientes no solamente físicos, sino en su gran mayoría lógicos, donde la ciberseguridad forma parte importante de la Industria 4.0 y que, dentro de este trabajo, se ha tomado en cuenta para instalar el servidor de servicios web.

Por otra parte, la responsabilidad social de trabajar de manera virtual y remota implica concientizar sobre la integración en un modelo de trabajo virtual, crear y obtener una infraestructura de internet que lleve a ciclos más cortos y capacidades de respuesta más rápidas. Porque una infraestructura de baja calidad no dará la adopción de la automatización digital.

Por tanto, se requiere gestionar un cambio integral de la diversidad tecnológica de las personas y es por ello que hay un reto de enfocar al personal en un ámbito de capacitación empresarial, que responda a las necesidades actuales y futuras en donde el mecanismo de capacitación tradicional va quedando fuera y es el reto de aumentar la diversidad de la fuerza laboral y cultural, así como generacional que incluya la aportación e intensificación en una mentalidad de trabajo responsable, continuo y aprendizaje de multidisciplinar habilidades que se enfoquen en proyectos creativos e inteligentes orientados a un pensamiento computacional.

IX. EVALUACIÓN DE RESULTADOS

El concepto de inteligencia es la parte más importante cuando hablamos de la Industria 4.0, es por ello que en este trabajo donde se implementa no solo el control que involucra la orden de activación o el paso a estar fuera de línea por medio de la APP diseñada para Android, se introduce el monitoreo donde el dispositivo Arduino Yun interactúa con el cliente o usuario, indicando el estado de la carga en activo o inactivo. Esto da el concepto de inteligencia, ya que con la implementación de sensores y actuadores no solo se puede controlar y monitorear, sino que el propio dispositivo puede decidir de acuerdo a parámetros mínimos, máximos y medios, cuál es la acción más adecuada ante un evento distinto al que fue creada la aplicación y el sistema, así como la funcionalidad de los dispositivos conectados.

Por ejemplo, en un ambiente donde el aire acondicionado de un centro de datos, se encuentre inactivo por algún apagón eléctrico y necesite ser restablecido físicamente mediante la activación de un botón, por medio de esta aplicación ya no será necesario que personal operativo se encuentre presente, ya que el dispositivo Arduino Yun, nos dará en primera instancia el estado de la carga en activo o inactivo, para su posterior activación de voltaje y corriente vía remota, ya sea por Ethernet y/o WiFi.

Además de ello, se puede interactuar con otros dispositivos sensores, para la posible activación de diversos actuadores que ayuden a identificar la problemática a resolver, como lo es el caso de alarmas sonoras, envío de mensajes y llamadas al celular, así como la activación de otro dispositivo de operación en caso de emergencia.

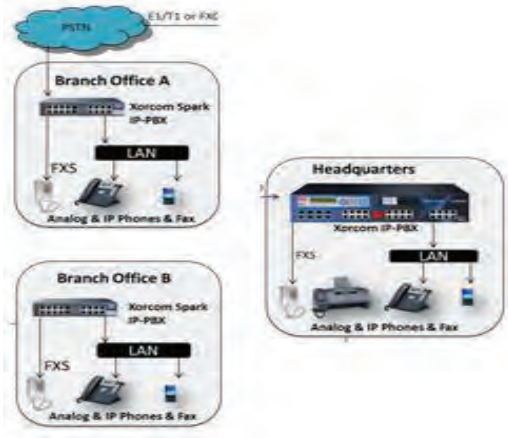


Fig. 4. Señalización y Comunicación de Protocolos.

X. Trabajo futuro

Hoy en día el hecho de pensar en una smart city, en México está cada vez más al alcance, debido a la integración de la industria y las múltiples aplicaciones innovadoras, con las que no solo las instituciones privadas empiezan a orientarse sino las instituciones públicas y gubernamentales también se están orientando, todo esto va creando un ecosistema donde un trabajo como el presentado de control y monitoreo a distancia de una carga digital o analógica, tiene cabida para ser parte de las aportaciones a la migración de mecanismos pasivos donde se les indicaba una orden y ahora a darle paso a la automatización donde los mecanismos interactúan brindando información de estado, para su posterior aplicación.

Es por eso que el remodelar sistemas productivos darán la alineación necesaria que trasladará al mundo de la Industria 4.0, para competir con el resto del mundo, optimizando procesos donde no implica la disminución de la parte laboral humana, sino el desarrollo de nuevas oportunidades de trabajo, donde se requiere personal con nuevos conocimientos para implementar expectativas de aportación en una re visualización del campo respecto a las nuevas revoluciones tecnológicas que están transformando al mundo.

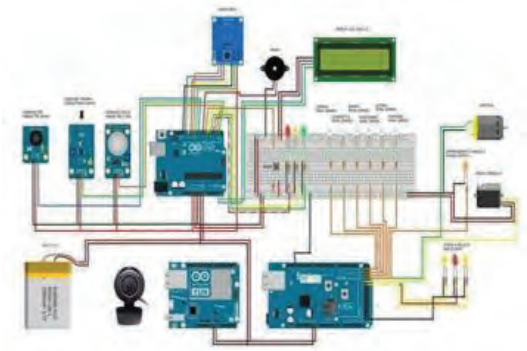


Fig. 5. Interacción inteligente en un ecosistema digital.

XI. MODELO DE NEGOCIO

El capital humano es la parte fundamental, porque las gestiones de dichas tecnologías son creadas por el talento humano que toma el reto de la expansión tecnológica mediante la vinculación del día a día al concepto de inteligencia digital, en el que las personas son más eficientes, asumiendo que la interconectividad virtual brinda profesionistas multi disciplinarios y también multi culturales, donde la competencia a nivel de conocimiento aplicado, será importante para colocarse dentro de un mercado global de negocios, donde el concepto de sistemas en tiempo real será vital en el manejo de todo, para entregar resultados en rendimiento, colaboración virtual, transferencia de operaciones e incremento de capacidades para enfrentar la convergencia de la innovación tecnológica.

XII. PROPUESTA DE MEJORA

Es importante resaltar que en el presente trabajo, se pretende implementar el software PBX- Asterisk, cuya finalidad es estandarizar la operación del sistema, para lograr una alta conexión con una gama muy diversa tanto de protocolos de comunicación con los que trabaja la tecnología de voz sobre protocolo de internet (VOIP) como lo son SIP, H323, MGCP, SKINNI, así como con los que trabaja la red conmutada telefónica, que es el protocolo Dahdi que sirve para interactuar con la telefonía tradicional y la telefonía digital.

Esto con la finalidad de ser heterogéneos a la hora de ingresar a la nube de internet y permanecer a la vanguardia en la integración y redundancia de servicios en un sistema de redes confiable y robusto dentro de un mundo físico y un mundo lógico, en los cuales la gestión más importante no está en los aspectos tecnológicos, sino en realizar un modelo que construya capacidades de aprovechamiento del análisis y puesta en marcha de los datos recopilados dentro de un proceso, para lograr optimizar ciclos de trabajo rumbo a la Industria 4.0.

XIII. CONCLUSIONES

En el presente trabajo se propone un Sistema basado en IoT mediante el cual se realiza el monitoreo de una carga eléctrica residencial o industrial. También debemos entender que el factor de cambio a considerar es la naturaleza cambiante laboral en el que nos encontramos, es por ello que se debe implementar nuevas ideas tecnológicas que den estrategias de negocios, los cuales afronten no solo el hecho de responder a una globalización, sino también que atienda al cambio climático, así como a los recursos naturales y los diferentes aportes que la revolución industrial 4.0 puede dar a mejorar dicho factor.

Así también tomar en cuenta la ética del nuevo mercado emergente con esta tecnología móvil y el buen manejo del Big Data para lograr una sustentabilidad de operación en los diferentes suministros de energías conjuntando el internet de las cosas. Logrando una estrategia de negocios de cualquier producto y servicio que ofrezca una experiencia realmente interactiva entre el mundo físico y el mundo lógico, dándonos una mejor calidad de vida humana y de preservación y mejora de nuestros recursos naturales.

Es por ello que, con base a los resultados obtenidos, se observa que el Sistema IoT propuesto representa una buena solución en el monitoreo remoto de cargas digital/analógicas para Smartphone. Porque se genera a través de la adopción de nuevas tecnologías una realidad exponencial de lo que vivimos cada día con un mundo interconectado a internet, en donde podemos enviar y recibir información, datos relevantes que permiten la interacción entre un mundo físico y un mundo virtual por medio de la digitalización de señales.

XIV. REFERENCIAS

[1] https://en.wikipedia.org/wiki/Internet_of_Things, Jun 25 (2016).
[2] Joo, D.Y and Kim, J.K.: Creative & active convergence model of IoT, Korea Institute for Industrial Economics & Trade, Korea (2014).
[3] Gauer, A.: Smart city Architecture and its applications based on IoT, Procedia computer science, (2015), Vol.52, pp.1089-1094.
[4] Bagula, A., Castelli, L and Zennaro, M.: On the design of smart parking networks in the smart cities: An optimal sensor placement model, Sensors, (2015), Vol.15, No.7, pp.15443- 15467.
[5] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, Digital Watermarking and Steganography, Morgan Kaufmann, Second Ed.
[6] Rodríguez Colín, R. (2007). Esquema de marcas de agua para imágenes médicas. Tesis de maestría, Instituto Nacional de Astrofísica, Optica y Electrónica, Tonantzintla, Puebla, México.
[7] Alejandra Menéndez Ortíz, Claudia Feregrino-Uribe and José Juan García- Hernández, "Reversible image watermarking scheme with perfect watermark and host restoration after a content replacement attack", The 13th International Conference on Security and Management, SAM'14, USA. Julio 2014.
[8] Bustio-Martínez, L., Coma-Pen˜a, Y., and Talavera-Bustamante, Arquitectura basada en plugins para el desarrollo de software científico. In Memorias de la II Conferencia Internacional de Ciencias Computacionales e Informa´ticas, CICCI 2013, La Habana, Cuba, 18-22 de marzo de 2013 (La Habana, Cuba, 2013), pp. 1–10.
[9] ComputerHoy. Los riesgos y peligros de los add-ons de fi- refox y chrome. https://computerhoy.com/noticias/internet/ riesgos-peligros- add-ons-firefox-chrome-12519.
[10] Dieterle, D. Basic Security Testing with Kali Linux 2. CreateSpace Independent Publishing Platform, 2016.
[11] RSA.com. Making sense of man-in-the-browser attacks. https://www.rsa.com/content/dam/rsa/PDF/Making_Sense_of_ Man_in_the_browser_attacks.pdf. Accessed: 2018-02-27.
[12] Symmantec. The elderwood project. http://www.c-cure.dk/Files/Datasheet/Symantec/Symantec%20the-elderwood-project.pdf. Ac- cessed: 2018-02-26.

Protección y Rompimiento del Pseudoanonimato de Blockchain

Víctor Reyes-Macedo*, Moisés Salinas-Rosales †
Instituto Politécnico Nacional
Centro de Investigación en Computación
Av. Juan de Dios Bátiz, Esq. Miguel Othón de Mendizábal
Nueva Industrial Vallejo, Gustavo A. Madero 07738
Ciudad de México
*vg.reyesmacedo@gmail.com,
†msalinasr@ipn.mx

Gina Gallegos-García
Instituto Politécnico Nacional
Escuela Superior de Ingeniería Mecánica y Eléctrica
Av. Santa Ana Nº 1000
San Francisco Culhuacan, Coyoacán 04260
Ciudad de México
ggallegos@ipn.mx

***Resumen*—A raíz del desarrollo de Bitcoin, la cadena de bloques o *blockchain*, que es la tecnología central de éste sistema de pagos, ha encontrado cada vez más espacios en los que su potencial puede ser aprovechado. Dichos espacios, han resultado particularmente atractivos a la industria, que ha adoptado esta tecnología en campos tan diversos como las finanzas, la medicina, la logística, el gobierno y la propiedad intelectual, por mencionar algunos. Sin embargo, aspectos tan importantes como la privacidad de las operaciones y el anonimato de sus participantes han sido dejados de lado. En este artículo, se presenta una revisión de los estudios que han evaluado propuestas para vencer el anonimato y la privacidad, y de los que han contribuido con propuestas para robustecer dichos servicios.**

***Index Terms*—Anonimato, bitcoin, blockchain, privacidad, seguridad .**

I. Introducción

En el año 2008, se presentó al mundo el sistema *Bitcoin*, un sistema de pago electrónico, el cual permite llevar a cabo transacciones de manera directa entre sus usuarios, sin la necesidad de involucrar a una entidad adicional de confianza, como es el caso de las instituciones bancarias. El funcionamiento de dicho sistema, en gran medida, se debe a la introducción de la cadena de bloques, conocida de manera global como *blockchain*, y que es descrita por Halpin y Piekarska en [1] como una lista de datos descentralizada y verificable criptográficamente, que garantiza la integridad de la información. Las aplicaciones de las cuales la tecnología *blockchain* forma parte al día de hoy, son numerosas y se presentan en diversos campos, siendo posible encontrar implementaciones en industrias dedicadas al cuidado de la salud, a las finanzas y servicios bancarios, elaboración de contratos inteligentes, licitaciones y servicios de gobierno, sistemas de votación electrónica y trazabilidad de insumos, entre otras [2]. El nivel y la velocidad de adopción del *blockchain* para una amplia gama de fines, pone de manifiesto la importancia del desarrollo de la investigación alrededor de la seguridad que ofrece este sistema, en particular, este documento aborda un enfoque centrado en los servicios de privacidad y anonimato. Por ello, este artículo presenta una revisión de las investigaciones que se han dedicado a estudiar estos aspectos, con la finalidad de ofrecer un panorama al respecto. El resto del artículo está organizado de la siguiente forma: la Sección II presenta un contexto del funcionamiento del blockchain de Bitcoin, la Sección III se centra en la revisión de estudios que han explotado el nivel de anonimato y privacidad del blockchain, mientras la sección IV presenta las propuestas de mejoramiento de estos servicios. La Sección V aborda los problemas abiertos al respecto, y en la Sección VI se presentan las conclusiones.

II. Una mirada a Bitcoin

Hablar de *blockchain*, frecuentemente conduce a hablar de Bitcoin para comprender la naturaleza de esta estructura de datos, cuya propuesta original, comprometió ligeramente la privacidad y el anonimato, con el objetivo de evitar el doble gasto y la falsificación durante las transacciones. Por ello, si bien las transacciones no se asocian, en primer instancia, a ninguna entidad, al completarse quedan registradas en el *blockchain* mediante identificadores, que consisten en cadenas alfanuméricas de entre 27 y 34 caracteres denominados *direcciones*. Así, una transacción consiste en el siguiente conjunto de datos:

- Dirección de origen: Son las direcciones que pagan un monto (puede ser más de una).
- Dirección de destino: Son las direcciones que reciben un monto (puede ser más de una).
- Monto: Cantidad de *bitcoins* que se pagan.
- Timestamp: Fecha y hora en que hizo la transacción.

Dichos datos, se almacenan en los bloques que conforman el *blockchain.* Estas características, demuestran que Bitcoin es un sistema de pago transparente, pese a que la identidad de los usuarios no es explícita. Por ello, diversas investigaciones se han centrado en los aspectos de privacidad y anonimato en el blockchain, con miras a fortalecer la seguridad en el rango de aplicaciones que tiene esta tecnología en la industria.

III. Rompiendo la privacidad y el anonimato

A menudo, los conceptos de privacidad y anonimato son confundidos, y pueden llegar a ser utilizados de manera indistinta. Al respecto, Bradbury señala en [3], que privacidad

significa ocultar el contexto, y anonimato significa ocultar al sujeto. En este sentido, al mejorar el servicio anonimato en *blockchain*, el objetivo será que el sujeto que interactúe en el sistema no sea identificable ni trazable, mientras que el servicio de privacidad deberá garantizar que la actividad de dicho sujeto no sea visible a terceros, es decir, la contraparte no debe tener acceso a los meta-datos de la interacción.

Al respecto, Kus Khalilov y Levi presentaron en [4], una taxonomía de los estudios de análisis de anonimato y privacidad en Bitcoin, la cual se muestra en la Figura 1.

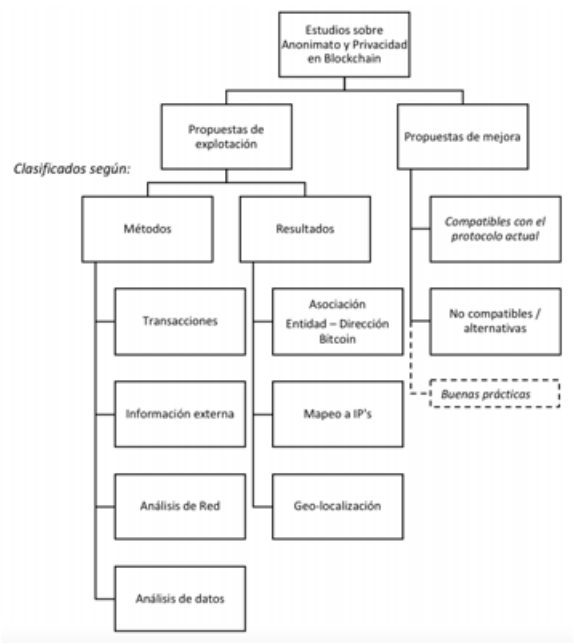


Figura 1. Taxonomía propuesta por Khalilov y Levi

Como se puede observar, proponen una clasificación con base en el tipo de resultados, la cual consiste en los siguientes aspectos:

- Identificación y asociación de una dirección Bitcoin con una persona o entidad, a partir de la información de la persona o entidad.
- Identificación y asociación de una identidad, a partir de la información de una dirección Bitcoin.
- Asociación de direcciones Bitcoin a direcciones IP.
- Asociación de direcciones Bitcoin que sean propiedad de un mismo usuario, mediante clústers.
- Geo-localización de direcciones Bitcoin.

En el mismo estudio, los autores abordan, además, los métodos que permiten llegar a los distintos tipos de resultados señalados arriba, a través de cuatro diferentes clases de métodos:

- Mediante transacciones
- Mediante uso de información externa
- Mediante el análisis del blockchain como red
- Mediante el análisis de los datos del blockchain

III-A. Mediante transacciones

Al interactuar con otro usuario, ya sea porque se compran o venden productos o servicios, necesariamente se conoce la dirección Bitcoin de la contraparte, por lo que ésta y su dirección pueden ser asociadas sin problema. Bajo este principio, Meiklejohn *et al.* [5] realizaron un *ataque de re-identificación*, en el cual llevaron a cabo operaciones con vendedores y proveedores de diversos servicios, con ello, lograron seguir el rastro de los pagos a través del *blockchain*, e identificar 344 transacciones con 87 entidades conocidas y 1070 direcciones.

Los autores, Kus Khalilov y Levi, incluyen en este apartado a los servicios de mixing o de anonimato, que tienen como objetivo mezclar los fondos de las transacciones de varias fuentes, y luego hacer los pagos correspondientes, para así hacer que dichos pagos no sean rastreables. Un análisis de este tipo de servicios y el nivel de anonimato que ofrecen, puede ser consultado en el trabajo de Möser *et al.* en [6].

III-B. Mediante el uso de información externa

En muchos casos, de manera voluntaria o involuntaria, los usuarios suelen revelar información acerca de la propiedad de sus direcciones Bitcoin, por ejemplo, para recibir un pago o donación. También es usual que en foros en línea, especializados o no en el tema, se publiquen direcciones que tienen altos índices de actividad -grandes montos durante amplios períodos, como el caso de los servicios de cambio de criptomonedas o *exchange*- y se asocien con las entidades correspondientes. Mediante este método, Reid y Harrigan identificaron algunas entidades asociadas a un presunto robo de 25000 BTC; además propusieron la heurística de *transacciones multi-entrada* para identificar a los propietarios de determinadas direcciones [7]. De la misma forma, Ron y Shamir asociaron 1088 transacciones de 83 direcciones con WikiLeaks, a partir de la dirección Bitcoin que la organización utiliza para recibir donaciones [8]. Por otra parte, Ortega desarrolló scripts para ligar direcciones Bitcoin con la identidad de sus usuarios, a través de la información que éstos proporcionaron en foros públicos [9].

Spagnuolo, posteriormente, presentó en [10] el *framework* BitIodine, el cual es un analizador del *blockchain*, que tiene la capacidad de agrupar las direcciones que son propiedad de la misma entidad en clusters, y etiquetarlos. Baumann *et al.* [11], lograron obtener las direcciones IP asociadas con las direcciones Bitcoin a través del sitio `blockchain.info`, con lo cual identificaron un conjunto de direcciones pertenecientes a MtGox, una antigua empresa operadora de criptomonedas. Finalmente, Lischke y Fabian reunieron información sobre 223,000 direcciones IP que fueron usadas en 15.8 millones de transacciones [12].

III-C. Mediante el análisis del blockchain *como red*

Este método utiliza la información de las transacciones, obtenida a través del análisis del tráfico en la red de Bitcoin o su infrastructura de red. Para ello, los enfoques que los

autores del estudio [4] identificaron, fueron clasificados en las siguientes categorías:

- *Utilizando transacciones retransmitidas de manera anormal*: Se definen patrones de comportamiento anormal, Koshy *et al.* en [13] utilizaron este método para relacionar direcciones Bitcoin con direcciones IP.
- *Utilizando el primer retransmisor de información*: Consiste en suponer que el primer nodo en informar de una transacción es el origen de ésta. No obstante, resulta poco efectivo comparado en el método anterior.
- *Utilizando nodos de entrada*: Esta información puede ser obtenida por los nodos al conectarse a la red, y de esta forma es posible identificar a los propietarios de las transacciones y relacionar las direcciones con sus respectivas IP's.
- *Estableciendo una dirección cookie para la huella del usuario*: permite asociar direcciones IP y direcciones Bitcoin del mismo usuario, de manera que es posible obtener una huella del propietario. El método fue propuesto por Biryukov y Pustogarov en [14].

III-D. Mediante el análisis de los datos del blockchain

Dado que la información y los metadatos de todas las transacciones generadas son de acceso público en el *blockchain*, el flujo de bitcoins es trazable. Dicha información puede ser consultada en sitios especializados como `blockchain.info`, o bien, para obtener una copia es suficiente con descargar algún cliente Bitcoin, como BitcoinCore, el cliente original. De esta forma, el estudio de Reid y Harrigan, fue el primero que abordó la privacidad y el anonimato en el *blockchain* de Bitcoin. Con la información disponible, representaron el flujo de pagos como una red dirigida, en la cual las direcciones tomaron el rol de nodos, y los enlaces indicaban los montos de las transacciones. Posteriormente, plantean que las direcciones que son propiedad del mismo usuario pueden ser identificadas mediante tres heurísticas: a) transacciones multi-entrada, b) direcciones de cambio y c) clustering basado en comportamiento

Androulaki *et al.* retomaron las heurísticas anteriores y llevaron a cabo una medición del anonimato, mediante una simulación del entorno Bitcoin. Ron y Shamir, por otro lado, aplicaron estas heurísticas para asociar las transacciones y direcciones relacionadas con *The Sheep Market Place*, un mercado negro en *deep web*, y al caso de *Dread Pirate Roberts*, supuesto creador del mercado negro conocido como *Silk Road*. Ortega *et al.* realizaron un análisis con cada heurística, con el cual demostraron que la forma más eficiente de asociar direcciones es mediante *transacciones multi-entrada*. Baumann *et al.* y, de forma independiente, Lischke y Fabián, llevaron a cabo un proceso similar. Meiklejohn *et al.* utilizaron las dos primeras heurísticas para ejecutar un ataque de reidentificación mediante información externa, mientras Spagnuolo desarrolló *BitIodine*, un framework que logra asociar y etiquetar direcciones en clusters, dicho framework tomó como caso de estudio las transacciones asociadas con *Dread Pirate Roberts* y el ataque del ransomware *CryptoLocker*. Mediante la aplicación de estas mismas heurísticas, Ober *et al.* descubrieron que el anonimato en Bitcoin se reduce a medida que el tamaño de las entidades que participan y el comportamiento de las operaciones se vuelven estacionarios. En el caso del estudio realizado por Dupont y Squicciarini, lograron geolocalizar a las entidades identificadas. Ferrin, al aplicar estas heurísticas, sugirió una forma de diferenciar a las direcciones de cambio, y Yanovich *et al.* reportaron que aproximadamente un 2.5 % de las transacciones pasan por un servicio de *mixing* para asegurar su anonimato. Por otra parte, Nick introdujo dos heurísticas nuevas, d) heurística de consumidor y e) heurística de cambio óptimo, que posteriormente fueron retomadas por Neudecker y Hartenstein [4].

Autor	Inicial (α)	Final (β)	Reducción ϕ
Reid y Harrigan	1,253,054	881, 678	0.7036
Androulaki *et al.*	1, 632,648	1, 069, 699	0.6552
Ron y Shamir	3,730, 218	2,460, 814	0.6597
Ortega*	1, 719, 312	32,956	0.0191
Ortega **	383, 990	32, 261	0.0840
Baumann*et al.*	17, 229, 680	No especificado	No especificado
Lischke y Fabián	17,229,680	No especificado	No especificado
Meiklejohnn	12, 056, 684	3, 383, 904	0.2806
Spagnuolo	18,153, 279	3, 383, 904	0.1864
Möser	No especificado	No especificado	No especificado
Ober *et al.*	12,711,115	No especificado	No especificado
Dupont y Squicciarini	38,886,789	17,472,156	2.225
Zhao y Guan	35,770,360	13, 062, 822	2.738
Fleder *et al.*	80, 030	54,941	1.456
Ferrin	112,070,000	No especificado	0.7036
Yanovich *et al.*	No especificado	No especificado	0.7036
Neudecker y Hartenstein	196,963, 722	$\sim$ 72 millones	02.735
Nick	60,880,000	No reportado	0.3

*Mediante análisis de transacciones con multientrada
**Mediante análisis de direcciones de cambio

Tabla I
MEDICIÓN DEL PARÁMETRO DE *reducción* DE LOS ESTUDIOS

Finalmente, Kus Khalilov y Levi, en [4], realizaron un análisis comparativo de los diferentes estudios que se han hecho al respecto, con énfasis en los métodos seguidos y los resultados obtenidos. La tabla I muestra una medición de la eficiencia de los estudios mencionados, al asociar direcciones con entidades. En dicha tabla, la primer columna señala al autor o autores del estudio en cuestión, la segunda, indica el número de direcciones con el cual inició el estudio y la tercera columna muestra el número de grupos de direcciones obtenidos. Para medir la eficiencia en el proceso de formación de grupos de direcciones, se propone el parámetro de *reducción* ϕ, definido por la ecuación 1.

$$\phi = \frac{\alpha}{\beta} \tag{1}$$

Donde α es el número de direcciones inicial, y β es el número de direcciones final, dado por el número de grupos

obtenidos. Este parámetro, no contempla las ventanas de tiempo correspondientes a la obtención de las muestras de direcciones, e indica que el estudio correspondiente tuvo un mejor desempeño respecto a otro si el valor es más cercano a cero. Este resultado se indica en la última columna de la tabla I. La leyenda *No especificado*, se debe a que el estudio no reporta la cantidad de direcciones con las que trabajó.

IV. Protegiendo la privacidad y el anonimato

Derivado de los estudios mencionados anteriormente, se han dado a conocer algunas medidas que tienen la capacidad de mejorar el nivel de privacidad que el sistema Bitcoin provee. En el estudio de Reid y Harrigan [7], los autores proporcionan las siguientes recomendaciones: a) generar nuevas direcciones para cada transacción, b) evitar revelar información que facilite la asociación de la dirección con la identidad del usuario, c) enviar fracciones de Bitcoin a una dirección propia de reciente creación y d) usar un servico de mixing confiable. Adicionalmente, Androulaki sugirió en [15], dividir el monto que se requiera para hacer un pago a una dirección propia, con el objetivo de evadir la heurística de direcciones de cambio. Por otro lado, Biryukov *et al.* [14] sugiere incrementar el tiempo requerido de computación para cada conexión, así como agregar retrasos aleatorios antes de completar las transacciones, para elevar la dificultad de la asociación de direcciones. Sin embargo se considera poco viable debido a que afectaría de manera negativa la funcionalidad del proceso. Ortega, además, propone en [9] el uso de diferentes monederos para distintos propósitos, de esta manera podría evitar la asociación de direcciones, y adicionalmente, incluir un pago lo suficientemente pequeño, con varios números en la parte fraccionaria, para complicar la asociación de direcciones de origen y destino que podría generar la heurística de dirección de cambio.

Más allá de las recomendaciones generales, que pueden ser consideradas como *buenas prácticas*, existe una variedad de propuestas que buscan mejorar los aspectos de seguridad que tienen que ver con anonimato y privacidad. Kus Khalilov y Albert Levi presentaron en [4], una clasificación de los estudios que ofrecen propuestas que pretenden proteger las operaciones en *blockchain* contra los intentos de identificación.

Dicha clasificación comprende dos ramificaciones principales: la primera, engloba los procesos que son compatibles con el protocolo actual de Bitcoin, sin la necesidad de implementar modificaciones de algún tipo, a los cuales denomina *backwards compatible*. Por otra parte, la segunda ramificación refiere a los procesos que no son compatibles con el protocolo actual, y para los cuales, sería necesario proponer alternativas a Bitcoin o bien, modificar su actual implementación, a esta rama se le denominó *not backwards compatible*.

Los procesos *backwards compatible*, básicamente consisten en alguna forma de mixing, técnica mediante la cual se cruzan los pagos de transacciones, para que no lleguen de forma directa [16] y que puede darse de forma centralizada o descentralizada. Mientras tanto, los métodos *not backwards compatible* se enfocan en: mezcla de direcciones ocultas, mezcla de propiedad, cifrado de datos y desintegración de datos.

Así mismo, presenta una clasificación en sub-categorías, tomando como criterios el enfoque, los protocolos y los métodos usados en cada estudio; además, ubican los resultados en una o varias de las siguientes categorías: a) rompimiento de relación entre direcciones de origen y destino en una transacción, b) rompimiento de relación entre transacciones, c) ocultamiento de montos de pago y d) ocultamiento de direcciones IP [4].

Finalmente, Andrew Miller presentó en [17], un framework que preserva la privacidad de los contratos inteligentes, denominado *Hawk*, con la intención de que cualquier programador sea capaz de programar un contrato inteligente sin tener que implementar funciones criptográficas, de manera que el compilador, automáticamente, compila el programa a un protocolo criptográfico entre los usuarios y el *blockchain*.

V. Problemas Abiertos

Kus Khalilov y Albert Levi consideran, en [4], que aunque existan propuestas de mejora al anonimato y a la privacidad, la expansión que experimentan los sistemas basados en Blockchain llevarán a mayores avances en los campos de la criptografía y la computación sobre los cuales habrá que dirigir los esfuerzos de investigación, principalmente en cuatro aspectos:

- *Desempeño:* Los métodos desarrollados para mejorar el nivel de privacidad y anonimato, deben incluir una sólida investigación respecto al desarrollo de métodos más efectivos, computacionalmente.
- *Seguridad:* Las propuestas criptográficas en torno al incremento de los aspectos de seguridad y privacidad deben ser examinados en busca de posibles vulnerabilidades.
- *Escalabilidad:* Un reto no menor, es conseguir las mejoras necesarias a los protocolos, sin comprometer la escalabilidad del sistema.
- *Anonimato y confianza:* Se debe buscar la forma de balancear el anonimato y la confianza, debido a que, a mayor nivel de anonimato, el nivel de confianza en el sistema es susceptible de disminuir, la razón de ello es la limitada capacidad que tendrían los usuarios de verificar el buen funcionamiento del mismo.

VI. Conclusiones

Como se ha podido observar, la idea original del *blockchain* implementada en Bitcoin, en el mejor de los casos provee pseudo-anonimato, contra el cual diversos estudios han dirigido esfuerzos para vencer, logrando en muchos casos identificar a las partes involucradas en las transacciones, mediante una variedad de métodos. Por otro lado, también existen estudios que se han dedicado a fortalecer el nivel de privacidad que dicha implementación ofrece, obteniendo dos tipos de resultados: aquellos que pueden implementarse sin necesidad de modificar el protocolo actual, y aquellos que, por el contrario, se plantean como una alternativa ya que proponen una modificación a dicho protocolo. No obstante, si bien éstas últimas logran su objetivo respecto a las garantías de seguridad, lo hacen

a cambio de poder de cómputo y riesgos a la integridad de la información. Adicionalmente, un reto interesante está en el desarrollo de métodos que permitan cuantificar y comparar el anonimato y privacidad obtenidos de los diferentes estudios, con la finalidad de diferenciar aquellos que logran mejores resultados. De esta forma, con miras a establecer protocolos que permitan implementar *blockchain* para detonar todo su potencial en la industria, es importante dirigir esfuerzos que concilien los aspectos de desempeño, seguridad, escalabilidad y confianza.

REFERENCIAS

[1] Harry Halpin and Marta Piekarska. Introduction to security and privacy on the blockchain. In *Security and Privacy Workshops (EuroS&PW), 2017 IEEE European Symposium on*, pages 1–3. IEEE, 2017.

[2] Michael Crosby, Pradan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman. Blockchain technology: Beyond bitcoin. *Applied Innovation*, 2:6–10, 2016.

[3] Danny Bradbury. Anonymity and privacy: a guide for the perplexed. *Network Security*, 2014(10):10–14, 2014.

[4] Merve Can Kus Khalilov and Albert Levi. A survey on anonymity and privacy in bitcoin-like digital cash systems. *IEEE Communications Surveys & Tutorials*, 2018.

[5] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. A fistful of bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 conference on Internet measurement conference*, pages 127–140. ACM, 2013.

[6] Malte Moser, Rainer Bohme, and Dominic Breuker. An inquiry into money laundering tools in the bitcoin ecosystem. In *eCrime Researchers Summit (eCRS), 2013*, pages 1–14. IEEE, 2013.

[7] Fergal Reid and Martin Harrigan. An analysis of anonymity in the bitcoin system. In *Security and privacy in social networks*, pages 197–223. Springer, 2013.

[8] Dorit Ron and Adi Shamir. Quantitative analysis of the full bitcoin transaction graph. In *International Conference on Financial Cryptography and Data Security*, pages 6–24. Springer, 2013.

[9] Marc Santamaria Ortega. The bitcoin transaction graph anonymity. 2013.

[10] Michele Spagnuolo, Federico Maggi, and Stefano Zanero. Bitiodine: Extracting intelligence from the bitcoin network. In *International Conference on Financial Cryptography and Data Security*, pages 457–468. Springer, 2014.

[11] Annika Baumann, Benjamin Fabian, and Matthias Lischke. Exploring the bitcoin network. In *WEBIST (1)*, pages 369–374, 2014.

[12] Matthias Lischke and Benjamin Fabian. Analyzing the bitcoin network: The first four years. *Future Internet*, 8(1):7, 2016.

[13] Philip Koshy, Diana Koshy, and Patrick McDaniel. An analysis of anonymity in bitcoin using p2p network traffic. In *International Conference on Financial Cryptography and Data Security*, pages 469–485. Springer, 2014.

[14] Alex Biryukov and Ivan Pustogarov. Bitcoin over tor isn't a good idea. In *Security and Privacy (SP), 2015 IEEE Symposium on*, pages 122–134. IEEE, 2015.

[15] Elli Androulaki, Ghassan O Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. Evaluating user privacy in bitcoin. In *International Conference on Financial Cryptography and Data Security*, pages 34–51. Springer, 2013.

[16] Malte Moser. Anonymity of bitcoin transactions. 2013.

[17] Andrew Miller. *Provable security for cryptocurrencies*. PhD thesis, 2016.

Un vistazo a la tokenización

Daniel Ayala Zamorano, Laura Natalia Borbolla Palacios, Ricardo Quezada Figueroa, Sandra Díaz-Santiago
Instituto Politécnico Nacional, ESCOM
Ciudad de México, México
{daz23ayala, ln.borbolla.42, qf7.ricardo, sdiazs}@gmail.com

***Resumen*—Un mecanismo alternativo para proteger datos sensibles, tales como los números de tarjetas bancarias, es la *tokenización*: consiste en reemplazar la información sensible por valores sustitutos llamados *tokens*. Al utilizar este mecanismo, se afirma que no es posible recuperar el dato original a partir del token; es decir, no se requiere de ningún mecanismo de seguridad para proteger a los tokens y, por tanto, si un atacante tiene acceso a ellos, no obtendrá ventaja alguna. Aunque esta solución resulta ideal, es necesario analizar, en términos de eficiencia y seguridad, cuáles son las opciones más adecuadas para generar tokens. Hasta el momento, se han propuesto varios algoritmos para hacerlo; sin embargo, no se tiene un análisis comparativo entre los mismos. En este artículo se explica en qué consiste la tokenización, cuáles son los algoritmos existentes para generar tokens y se muestra una comparación de desempeño con base en una implementación propia de estos. Finalmente, es importante señalar que los algoritmos analizados están basados en primitivas criptográficas cuya seguridad ya ha sido probada.**

***Palabras clave*—tokenización, criptografía simétrica, seguridad web**

I. Introducción

Cuando el comercio a través de Internet comenzó a popularizarse, los fraudes de tarjetas bancarias se convirtieron en un problema alarmante: según [13], en 2001 se tuvieron pérdidas de 1.7 mil millones de dólares y para 2002 aumentaron a 2.1 mil millones. En este contexto, el *Payment Card Industry Security Standard Council (PCI SSC)*, integrado por las principales compañías de tarjetas de crédito, desarrolla el estándar *Payment Card Industry Data Security Standard (PCI DSS)* [16], con el propósito de especificar mecanismos de seguridad para proteger los datos sensibles de las tarjetas de crédito. Sin embargo, satisfacer los requerimientos establecidos en dicho estándar es sumamente difícil, especialmente para los negocios pequeños y medianos. Esto se debe a que la información sensible debe protegerse en donde sea que se encuentre: al almacenarla, transmitirla y/o procesarla. A pesar de la publicación del estándar en 2004, las grandes filtraciones de datos no han cesado: *TJX* en 2006, *Hannaford Bros.* en 2008, *Target* en 2013 y *Home Depot* en 2014, por mencionar algunos ejemplos [13].

Ante este escenario surge un nuevo paradigma, denominado *tokenización*, el cual consiste en reemplazar los datos sensibles por un *token*, es decir, un valor numérico o alfabético que no tiene relación alguna con el dato original. En este paradigma, la información se concentra en un solo lugar para hacer la tarea de protección más sencilla; así, cuando se ingresa un nuevo valor, v.g. un número de tarjeta de un usuario, se genera un token ligado a esa información, el cual se usa en todo el sistema y la información confidencial se protege en un solo lugar. Un posible adversario con acceso a los tokens no podrá obtener la información sensible a partir de estos.

Una de las ventajas de la tokenización es que puede verse como un sistema autónomo, independiente al sistema principal; de esta manera se establece una separación de responsabilidades: el sistema principal realiza la operación del negocio (por ejemplo, una tienda en línea) y el sistema tokenizador se dedica a la protección de la información sensible. Hoy en día, varias compañías ofrecen servicios de tokenización que permiten que los comerciantes se liberen casi por completo de cumplir con el PCI DSS. En la Figura 1, se muestra una distribución bastante común para un comercio en línea: el sistema tokenizador guarda la información sensible en su base de datos y se encarga de realizar las transacciones bancarias.

Aunque esta solución parece apropiada, aún es necesario responder preguntas tales como ¿cuáles son los mecanismos para generar tokens?, ¿cuál es su nivel de desempeño?, ¿cuáles son las implicaciones de seguridad al utilizar algún algoritmo en particular? Desafortunadamente, la tokenización se ha visto rodeada por una nube de desinformación desde sus inicios; la falta de una definición formal permitió que las campañas publicitarias de las empresas tokenizadoras difundieran información imprecisa: se suele mencionar que la tokenización y la criptografía no están relacionadas directamente, o bien, que la primera es una alternativa (y no una aplicación) de la segunda. Por ejemplo, lo único que *Shift4* dice con claridad sobre sus tokens, es que se trata de valores aleatorios, únicos y alfanuméricos [19]; para *Braintree*, la única manera de generar tokens es por métodos aleatorios [6]; finalmente, para *Securosis* los tokens son valores aleatorios que nada tienen que ver con la criptografía [18]; es fácil observar que la mayoría de las empresas trata a sus métodos como secretos de compañía, esperando que el trato entre cliente y proveedor esté basado en la confianza y no en la comparación de los propios métodos tokenizadores.

Afortunadamente, ya se han dado los primeros pasos para responder a las preguntas antes planteadas. Hasta el momento se han propuesto diversas soluciones para generar tokens, las cuales están basadas en primitivas criptográficas y también se ha comenzado a analizar la seguridad de tales soluciones. El presente artículo ofrece una breve descripción de los principales algoritmos para generar tokens, los cuales están basados en funciones hash, cifrados por bloque, cifrados que preservan el formato, entre otros. También se analiza la eficiencia de los mismos, con la finalidad de ofrecer un punto de comparación

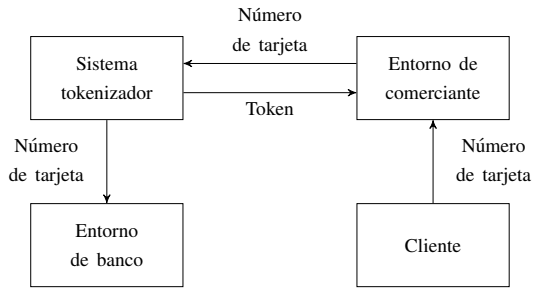


Figura 1. Arquitectura típica de un sistema tokenizador.

entre ellos.

En la Sección II se definen las primitivas criptográficas que utilizan los distintos algoritmos para generar tokens; en la Sección III, se da una breve descripción de los métodos de tokenización implementados. Finalmente, en la Sección IV, se presentan los resultados de las comparaciones de desempeño realizadas y se concluye con una discusión alrededor del tema.

II. Preliminares

II-A. Notación

Se denotará a todas las cadenas de bits de longitud n como $\{0,1\}^n$ y a las cadenas de longitud arbitraria como $\{0,1\}^*$. Para una cadena de símbolos x sobre un alfabeto arbitrario, $|x|$ simboliza la longitud de la cadena.

II-B. Primitivas criptográficas

Un cifrado por bloques se define como una función $e : \mathcal{M} \times \mathcal{K} \to \mathcal{C}$ donde $\mathcal{M} = \mathcal{C} = \{0,1\}^n$, $\mathcal{K} = \{0,1\}^k$, n, es el tamaño del bloque y k, el tamaño de la llave [14].

Los modos de operación permiten extender la funcionalidad de los cifrados por bloque para poder operar sobre bloques de información de tamaño arbitrario. Más formalmente, un modo de operación es un procedimiento que recibe como entrada un mensaje de longitud arbitraria $M \in \{0,1\}^*$, una llave $K \in \{0,1\}^k$, un vector de inicialización $IV \in \{0,1\}^v$ y da como salida un texto cifrado $C \in \{0,1\}^*$ [8].

Una función hash criptográfica asocia cadenas de longitud arbitraria a cadenas de longitud fija: $H : \{0,1\}^* \to \{0,1\}^h$, donde h es la longitud de la cadena de salida, también denominada resumen o digesto. No debe ser factible recuperar el mensaje a partir de su valor hash, ni encontrar dos mensajes que produzcan el mismo hash [14].

Un código de autenticación de mensaje (MAC, *Message Authentication Code*) es una primitiva criptográfica que provee integridad. Se define como una tupla de tres algoritmos: generación de claves, generación de la etiqueta y verificación de la etiqueta. El algoritmo para generar la etiqueta recibe como entrada una llave $K \in \mathcal{K}$ y un mensaje $M \in \{0,1\}^*$; como salida se obtiene una etiqueta $\tau \in \{0,1\}^t$. El algoritmo de verificación calcula una etiqueta τ' a partir del mensaje M y la llave K, y la compara con la etiqueta τ: si ambas son iguales, se dice que el mensaje no ha sido modificado. Aunque existen varias maneras de generar MAC, en este trabajo solamente se utiliza solamente CBC-MAC [20].

Las redes Feistel son cifrados iterativos que transforman un texto en claro de $2t$ bits denominado (L_0, R_0), en donde L_0 y R_0 son bloques de t bits, en un texto cifrado (R_r, L_r) a través de un proceso de r rondas. Existen dos generalizaciones de este concepto, las redes alternantes y las redes desbalanceadas; ambas permiten modificar el tamaño de las mitades izquierda y derecha: $1 \leq |L_n| \leq 2t$ y $|R_n| = 2t - |L_n|$ [17].

Un cifrado que preserva el formato (en inglés *Format-preserving Encryption*, FPE) es un cifrado simétrico en donde el mensaje en claro y el mensaje cifrado mantienen un formato común. Formalmente, de acuerdo a lo definido en [3], se trata de una función $E : \mathcal{K} \times \mathcal{N} \times \mathcal{T} \times \mathcal{X} \to \mathcal{X}$, en donde los conjuntos $\mathcal{K}$, $\mathcal{N}$, $\mathcal{T}$, $\mathcal{X}$ corresponden al espacio de llaves, espacio de formatos, espacio de *tweaks* y el dominio, respectivamente. El proceso de cifrado de un elemento del dominio con respecto a una llave K, un formato N y un *tweak* T se escribe como $E_K^{N,T}(X)$. El proceso inverso es también una función $D : \mathcal{K} \times \mathcal{N} \times \mathcal{T} \times \mathcal{X} \to \mathcal{X}$, en donde $D_K^{N,T}\left(E_K^{N,T}(X)\right) = X$.

III. Algoritmos tokenizadores

En el presente artículo se trata a la generación de tokens como un servicio, ver Figura 1, por lo que la interfaz para los procesos de tokenización y detokenización, desde el punto de vista del usuario, se define como sigue: el proceso para generar un token es una función $E : \mathcal{X} \to \mathcal{Y}$ y el proceso para recuperar al número de tarjeta es simplemente la función inversa $D : \mathcal{Y} \to \mathcal{X}$, en donde $\mathcal{X}$ y $\mathcal{Y}$ son los espacios de números de tarjetas y tokens, respectivamente. Los números de tarjetas bancarias cuentan con entre 12 y 19 dígitos, y están normados por el estándar ISO/IEC-7812 [12].

III-A. Clasificación del PCI SSC

El PCI SSC establece en sus guías de tokenización la siguiente clasificación para los algoritmos tokenizadores [15]:

- Métodos reversibles. Aquellos para los cuales es posible obtener el número de tarjeta a partir del token.
  - Criptográficos. El proceso de tokenización está basado en un esquema de cifrado simétrico que usa el número de tarjeta y una llave para obtener un token. El proceso de detokenización solicitará el token y la misma llave para recuperar el número de tarjeta.
  - No criptográficos. Se requiere una base de datos para guardar las relaciones entre números de tarjetas y tokens; el proceso de detokenización es una consulta a la base de datos.
- Métodos irreversibles. Aquellos en los que no es posible obtener el número de tarjeta original a partir del token.
  - Autenticable. Permiten validar cuando un token dado corresponde a un número de tarjeta.
  - No autenticable. No permiten hacer la validación anterior.

III-B. Algoritmos implementados

En esta sección se describen brevemente algunas de las soluciones que han sido propuestas por la comunidad académica para generar tokens. Las dos primeras son cifrados que preservan el formato que ya forman parte de los estándares del NIST (*National Institute of Standards and Technology*) [10]. La ventaja de estos mecanismos es que no se requiere de una base de datos para recuperar el número de tarjeta de crédito, basta con descifrar el token.

FFX (*Format-preserving Feistel-based Encryption*) fue presentado en [4] por Bellare, Rogaway y Spies. Este algoritmo permite cifrar cadenas de cualquier longitud en cualquier alfabeto; en particular, se consideran alfabetos binarios y alfabetos decimales, denominados A2 y A10, respectivamente. FFX A10 usa una red Feistel alternante junto con una adaptación de AES-CBC-MAC (usada como función de ronda) para lograr preservar el formato. Brier, Peyrin y Stern propusieron el algoritmo BPS [7] que se conforma de 2 partes: un cifrado interno BC que cifra bloques de longitud fija y un modo de operación especial, encargado de extender la funcionalidad de BC y de permitir cifrar cadenas de mayor longitud.

En 2016, Díaz et. al. [9] analizaron el problema de la generación de tokens desde el punto de vista criptográfico y propusieron un algoritmo (TKR) que no está basado en cifrados que preservan el formato. Hasta antes de la publicación de este documento, los únicos métodos para generar tokens cuya seguridad estaba formalmente demostrada eran los basados en cifrados que preservan el formato. El algoritmo propuesto usa un cifrado por bloques para generar tokens pseudoaleatorios y almacena en una base de datos la relación original de estos con los números de tarjetas. El proceso de detokenización es simplemente una consulta sobre la base de datos.

En 2017, Longo, Aragona y Sala [1] propusieron un algoritmo que denominaron *híbrido reversible* (AHR) que está basado en un cifrado por bloques y utiliza una base de datos para almacenar las relaciones entre número de tarjeta y token. Las entradas del algoritmo son la parte del número de tarjeta a cifrar y una entrada adicional (por ejemplo, la fecha) que permite que se tengan varios tokens relacionados con la misma tarjeta. Como se desea obtener un token que tenga el mismo número de dígitos que la tarjeta ingresada, se utiliza un método llamado *caminata cíclica* [5] para asegurarse de que el texto cifrado pertenezca al espacio del texto en claro.

Probablemente el método más directo para generar tokens es mediante un DRBG (*Deterministic Random Bit Generator*). La idea es producir una cadena binaria aleatoria con un DRBG e interpretarla para que tenga el formato de un token. Para este trabajo se hizo la implementación de dos DRBG: uno basado en funciones hash y otro basado en un cifrado por bloques; ambos definidos en el estándar del NIST 800-90A [2].

El método que utiliza como mecanismo interno a una función hash consiste en ir concatenando de forma consecutiva los valores hash derivados de la semilla e ir incrementando el valor de esta. El método basado en un cifrado por bloques utiliza el modo de operación CTR, en donde la semilla juega el papel de vector de inicialización. En ambos casos, la seguridad se basa en que la semilla sea un valor secreto.

Según la clasificación del PCI DSS, FFX y BPS son algoritmos reversibles criptográficos, ya que al ser cifrados que preservan el formato, funcionan como esquema de cifrado simétrico. TKR, AHR y DRBG son, contradictoriamente, reversibles no criptográficos, pues necesitan de una base de datos para guardar las relaciones tarjeta-token.

Tabla I
COMPARACIÓN DE TIEMPOS DE TOKENIZACIÓN.

	Tokenización (μs)	Detokenización (μs)
FFX	83	61
BPS	573	315
TKR	4648	281
AHR	5554	657
DRBG	4649	431

IV. RESULTADOS Y CONCLUSIONES

En la Tabla I y la Figura 2a se muestran los resultados en tiempo de las ejecuciones de los algoritmos presentados en la Sección III-B. Estos se llevaron a cabo en una computadora con las siguientes características:

- **Procesador:** Intel i5-7200U (2.5 GHz) de 4 núcleos.
- **Sistema operativo:** Arch Linux, kernel 4.17.
- **Base de datos:** MariaDB 10.1.
- **Compilador:** GCC 8.1.1.

El procesador utilizado soporta los conjuntos de instrucciones de Intel AES-NI y RD-SEED [11]. Los algoritmos tokenizadores que usan un cifrado por bloques utilizan una implementación de AES con las instrucciones a nivel de hardware. El DRBG se implementó haciendo uso de la instrucción RD-RAND como fuente de entropía.

La comparación de la Figura 2a muestra como los dos algoritmos reversibles, FFX y BPS, son considerablemente más rápidos que los tres irreversibles: TKR, AHR y DRBG. Los reversibles están en el rango de 60 a 170 microsegundos, mientras que los irreversibles están en alrededor de los 5500 microsegundos. También es posible observar que, para los métodos irreversibles, el proceso de detokenización es mucho más rápido que la generación de tokens. Estos dos resultados dejan ver un poco la carga de las operaciones en los métodos irreversibles: la tokenización involucra una consulta a la base, la generación del token y una inserción; la detokenización solamente es una consulta.

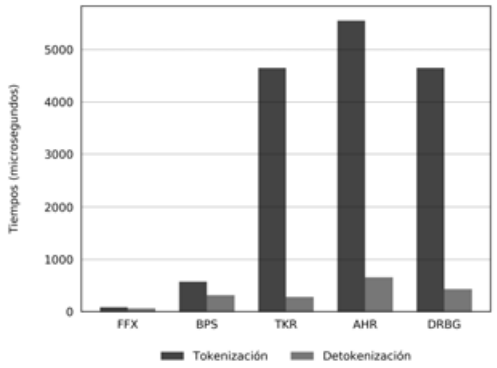
El que FFX y BPS sean más rápidos puede resultar un poco contraintuitivo, pues la generación de tokens reversibles involucra más operaciones; es por esto que en la Figura 2b se muestran los tiempos de la generación de tokens, sin tomar en cuenta tiempos de acceso a base de datos. En este caso, el más veloz es DRBG, seguido de cerca por TKR y AHR; los dos reversibles van al último.

Además de los tiempos de ejecución, también es importante señalar que los irreversibles, al operar como funciones de un

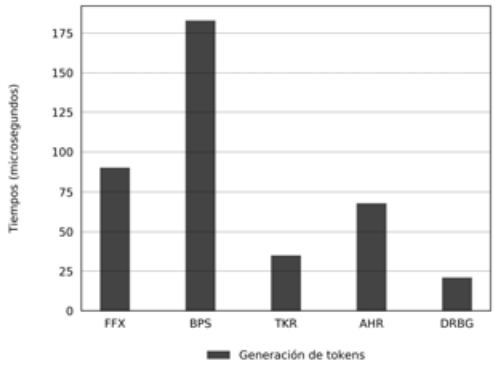
solo sentido, son más seguros que los reversibles: un atacante con acceso a la llave de cifrado puede obtener el número de tarjeta correspondiente si se trata de un método reversible, mientras que con un método irreversible necesita también acceso a la base de datos.

La denominación *no criptográficos*, de la clasificación del PCI DSS resulta totalmente confusa, pues en realidad todos los métodos conocidos que caen en esa categoría utilizan primitivas criptográficas. La segunda categoría (irreversibles) carece de utilidad para aplicaciones que procesan pagos con tarjetas de crédito, pues la habilidad de regresar al número de tarjeta a partir de su token es uno de los requerimientos principales para los sistemas tokenizadores. Por lo anterior, en este trabajo se propone una clasificación distinta:

- Métodos criptográficos. Todos aquellos basados en primitivas criptográficas.
  - Reversibles. Usan un esquema de cifrado simétrico. El mecanismo de tokenización cifra el número de tarjeta y la detokenización descifra el token para obtener el número de tarjeta original.
  - Irreversibles. Hacen uso de algoritmos criptográficos para generar el token y herramientas externas, como una base de datos, para guardar las relaciones entre tokens y números de tarjetas.
- Métodos no criptográficos. Aquellos métodos que no necesitan herramientas relacionadas con la criptografía; por ejemplo, un generador de números realmente aleatorio (TRNG, *True Random Number Generator*).



(a) Tokenización y detokenización



(b) Generación de tokens

Figura 2. Comparaciones de tiempos.

Agradecimientos

Los autores agradecen el apoyo del Instituto Politécnico Nacional, a través del proyecto multidisciplinario SIP 1917, módulo 20180775.

Referencias

[1] R. Aragona, R. Longo, and M. Sala. Several proofs of security for a tokenization algorithm. *Appl. Algebra Eng. Commun. Comput.*, 28(5):425–436, 2017.

[2] E. Barker and J. Kelsey. NIST special publication 800-90a - recommendation for random number generation using deterministic random bit generators, 2015.

[3] M. Bellare, T. Ristenpart, P. Rogaway, and T. Stegers. Format-preserving encryption. In M. J. J. Jr., V. Rijmen, and R. Safavi-Naini, editors, *Selected Areas in Cryptography*, volume 5867 of *Lecture Notes in Computer Science*, pages 295–312. Springer, 2009.

[4] M. Bellare, P. Rogaway, and T. Spies. The FFX mode of operation for format-preserving encryption. NIST submission, 2010. http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ffx/ffx-spec.pdf.

[5] J. Black and P. Rogaway. Ciphers with arbitrary finite domains. In B. Preneel, editor, *CT-RSA*, volume 2271 of *Lecture Notes in Computer Science*, pages 114–130. Springer, 2002.

[6] Braintree. Tokenization secures CC data and meet PCI compliance requirements. https://www.braintreepayments.com/blog/using-tokenization-to-secure-credit-card-data-and-meet-pci-compliance-requirements/. Consultado en marzo de 2018.

[7] E. Brier, T. Peyrin, and J. Stern. BPS: a format-preserving encryption proposal. NIST submission, 2010. http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/bps/bps-spec.pdf.

[8] D. Chakraborty and F. Rodríguez-Henríquez. Block cipher modes of operation from a hardware implementation perspective. In *Cryptographic Engineering*, pages 321–363. 2009.

[9] S. Diaz-Santiago, L. M. Rodríguez-Henríquez, and D. Chakraborty. A cryptographic study of tokenization systems. *Int. J. Inf. Sec.*, 15(4):413–432, 2016.

[10] M. Dworkin. NIST special publication 800-38g - recommendation for block cipher modes of operation: Methods for format-preserving encryption, 2016.

[11] G. Hofemeier and R. Chesebrough. Introduction to intel AES-NI and intel secure key instructions.

[12] International Organization for Standarization. *ISO/IEC 7812*. 5 edition, 2017.

[13] J. S. Kiernan. Credit card and debit card fraud statistics. https://wallethub.com/edu/credit-debit-card-fraud-statistics/25725/. Consultado en marzo de 2018.

[14] A. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[15] Payment Card Industry Security Standards Council. Tokenization product security guidelines – irreversible and reversible tokens, 2015.

[16] Payment Card Industry Security Standards Council. Data security standard - version 3.2, 2016.

[17] B. Schneier and J. Kelsey. Unbalanced feistel networks and block cipher design. In *Fast Software Encryption, Third International Workshop, Cambridge, UK, February 21-23, 1996, Proceedings*, pages 121–144, 1996.

[18] Securosis. Understanding and selecting a tokenization solution. https://securosis.com/assets/library/reports/Securosis_Understanding_Tokenization_V.1_.0_.pdf. Consultado en febrero de 2018.

[19] Shift4 Payments. The history of truetokenization. https://www.shift4.com/dotn/4tify/trueTokenization.cfm. Consultado en agosto de 2018.

[20] D. Whiting, R. Housley, and N. Ferguson. Counter with CBC-MAC (CCM). *RFC*, 3610:1–26, 2003.

Simulación de una Blockchain utilizando la API Bouncy Castle

Álvaro Zavala, Member, IEEE
Unidad de Tecnología Informática
Universidad de Sonsonate
Sonsonate, El Salvador
alvarohz@gmail.com

Leonel Maye
Unidad de Informática
Ministerio de la Defensa Nacional
Sonsonate, El Salvador
maye@mdn.mil.sv

***Resumen*—*Blockchain* es una bitácora de acontecimientos digitales descentralizada, asegurada mediante criptografía y que solo puede ser actualizada por consenso de la mayoría de participantes en el sistema en el que está aplicado. Se garantiza que esta bitácora no pueda ser alterada a favor de unos pocos por medio de técnicas criptográficas. En este artículo se reporta cómo se puede simular una *blockchain* haciendo uso de la API Bouncy Castle mediante la cual se proveen las siguientes primitivas criptográficas: funciones hash y firma digital. Además se hace uso de una base de datos en MySQL en donde se generan todas las transacciones y un programa desarrollado en C# para minería, es decir, que por medio de éste se verifican las transacciones para que sean adheridas a la *blockchain*. Finalmente, otra aportación es una plataforma web que se encuentra escrita en C# donde se pueden efectuar transacciones entre usuarios y consultar la *blockchain*.**

***Index Terms*—Blockchain, Criptomoneda, SHA, Cartera, Transacción, Minería**

I. Introducción

Una cadena de bloques (*blockchain*) es una lista de registros en continuo crecimiento, llamados bloques, que están vinculados y asegurados mediante criptografía. Cada bloque contiene típicamente un hash criptográfico del bloque anterior, una marca de tiempo y datos de las transacciones. Por diseño, una cadena de bloques es resistente a la modificación de los datos. Es una bitácora abierta y distribuida que puede registrar transacciones entre dos partes de manera eficiente y de manera verificable y permanente [1]. Actualmente una *blockchain* está ampliamente utilizada en criptomonedas y ésta es solamente una de las aplicaciones que puede proporcionarnos una cadena de bloques. Porque su potencial es mayor, puede ser usada en el campo de bases de datos, en sistemas de gestión de activos digitales, notarios distribuidos, contratos inteligentes, al ser *blockchain* una red inalterable y fiable de datos, se podría utilizar para llevar la gestión contable de las empresas y gobiernos, para que se pueda ver si cumplen con las normas vigentes [2]. Uno de los sectores que estaban en contra de las criptomonedas es la banca, sin embargo, ahora se encuentran invirtiendo para conseguir cadenas de bloques propias con el fin de mejorar la fiabilidad de sus transacciones [3]. En este artículo se propone la simulación de una *blockchain* como la que utiliza Bitcoin a partir del uso de la API Bouncy Castle, la cual es una librería que tiene todos los algoritmos criptográficos necesarios para el proyecto, se ha optado por generar una simulación para comprender cómo funciona disminuyendo la complejidad. Los componentes desarrollados son: a) una base de datos para almacenar la *blockchain* con todas las operaciones, b) un programa que permite realizar la minería, comprobando las operaciones y así poder insertarlas en la *blockchain*, c) una plataforma web, un sitio dónde los usuarios puedan crear sus propias carteras y hacer operaciones entre ellos.

II. Preliminares

La seguridad de las criptomonedas está basada en criptografía de llave pública (Curvas Elípticas) e implementan la *blockchain* para resolver el problema del doble gasto y prevenir la modificación de transacciones previas, a continuación, se describen los bloques más importantes para esta tecnología.

II-A. Función Hash

Una hash es una función computacionalmente eficiente que relaciona cadenas binarias de longitud arbitraria a cadenas binarias de longitud fija, denominadas digestos [4]. Algunos de los usos criptográficos de las funciones hash son las firmas digitales y la integridad de datos.

II-B. Firma Digital

La firma digital es el resultado de una transformación criptográfica de datos que, cuando se implementa correctamente, proporciona un mecanismo para verificar la autenticación de origen, la integridad de los datos y el no repudio del signatario. Un algoritmo de firma digital incluye un algoritmo de generación de llaves, un algoritmo de firma y un algoritmo de verificación de firma. Un signatario usa el algoritmo de generación de firma y su llave privada para generar una firma digital sobre un mensaje; un verificador utiliza el proceso de verificación y la llave pública del signatario para verificar la autenticidad de la firma [4].

II-C. Cartera (Wallet)

Una Billetera o Wallet es un repositorio de direcciones de depósito, cada dirección tiene asociada un par de llaves privada y pública [5]. Las direcciones se derivan a partir de los digestos de las llaves públicas.

II-D. Transacciones

Se define una transacción como una transferencia de valor de un ente a otro, siendo este último conocido como beneficiario, entiéndase por ente a una dirección. El modelo se basa en un libro de contabilidad, la transferencia da como resultado saldos en las salidas [6]. El problema, por supuesto, es que el beneficiario no puede verificar que el ente que le transfiere no haya gastado dos veces la misma moneda. La *blockchain* es usada para solucionar el problema del doble gasto y prevenir la modificación de transacciones previas.

II-E. Bloques

Cada bloque representa un conjunto de transacciones confirmadas, que se va uniendo a la cadena, está formado por: Un código hash que enlaza el bloque anterior, las transacciones y otro hash que enlazará el siguiente bloque [6]. Cada bloque debe de ser validado por el resto de computadoras de la red, entre ellos los mineros.

II-F. Servidor de estampa de tiempo

Un servidor de estampa de tiempo trabaja tomando el hash de un bloque de ítems para sellarlos en el tiempo y notificar públicamente su hash. Cada estampa de tiempo incluye la estampa de tiempo previa en su hash, formando una cadena, con cada estampa de tiempo adicional reforzando al que estaba antes [5]. Básicamente es la *blockchain*

II-G. Mineros

El trabajo de los mineros consiste en que estos bloques sean validados, crear el hash correspondiente y unirlo al resto de la cadena de bloques. Cuando se realizan varias transferencias, estos mineros (computadoras) las van confirmando y las van añadiendo a lo que sería el siguiente bloque de la cadena, una vez tienen un bloque completo, toman el hash del último bloque para generar el hash del siguiente, de esta forma se asegura que el hash que se añadirá será único e intransferible (si se intentara insertar un bloque falsificado, el hash que produciría sería diferente del que debería de ir almacenado a la cadena y sería identificado como falso) [7]. En Bitcoin, cada vez que un minero crea un hash con éxito, se le recompensa con monedas virtuales.

II-H. Red (nodos)

Son las diferentes computadoras conectadas en la red de *Blockchain*. Cualquiera puede descargarse la cartera de *Blockchain* (por ejemplo, de Bitcoins) y contribuir a que la red sea más segura. Cada vez que se confirma un bloque nuevo en la red, se comunica a todos los nodos para que vuelvan a actualizar su cartera [7]. En el caso de que algún nodo quiera realizar una transacción, su *blockchain* local deberá estar actualizado y sincronizado con el resto de nodos.

Se debe mencionar que los conceptos anteriores son independientes de la moneda criptográfica a la que se haga referencia, por lo general estas se diferencian por los algoritmos criptográficos empleados para la generación de llaves, la firma, el cálculo de hashes.

III. Estado del Arte

Existen muchos frameworks para implementar *blockchains* a partir de las aplicaciones que esta tiene, entre ellos los siguientes:

- **Hyperledge** (o proyecto Hyperledger) es una plataforma código abierto para *blockchain*, iniciado en diciembre de 2015 por la Fundación Linux, para apoyar a los ledgers distribuidos basados en la *blockchain*. Los objetivos del proyecto son aunar un número de esfuerzos independientes para desarrollar estándares y protocolos abiertos, así como proporcionar un marco modular que soporte componentes diferentes para usos diferentes [8].
- **Ethereum** es una plataforma open source, descentralizada que permite la creación de acuerdos de contratos inteligentes entre pares, basada en el modelo *blockchain*. Cualquier desarrollador puede crear y publicar aplicaciones distribuidas que realicen contratos inteligentes. Ethereum también provee una criptomoneda que se llama 'ether' [9].
- **Bouncy Castle** es una colección de APIs utilizados en criptografía. Tiene versiones para los lenguajes Java y C#. La API de bajo nivel está optimizada para gestionar eficientemente los algoritmos criptográficos, de forma que se puedan usar en entornos de bajos recursos y provee todas las herramientas criptográficas involucradas para crear una *blockchain* [10].

IV. Metodología

Para el desarrollo de la aplicación y la determinación de requerimientos se utiliza como referencia la metodología ágil SCRUM, y basándonos en algunos de sus artefactos como: Pila del Producto, Pila del sprint y Sprint. [11]

IV-A. Visión del producto

La aplicación debe permitir a los usuarios el manejo de sus carteras electrónicas o wallets:

- Generar las carteras electrónicas
- Generación de usuarios.
- Puesta a disposición de los mineros, una cola de transacciones que permitan a los mineros cálculos los valores válidos para las nuevas transacciones.
- Guardado de la *blockchain*, como mecanismo de seguridad de las transacciones.
- Evitar el doble gasto.

V. Desarrollo del proyecto

La aplicación se divide en dos partes: aplicación de escritorio para la minería y aplicación web para el manejo de las carteras electrónicas, ambas programadas con el API Bouncy Castle, tanto para el cálculo de los picadillos y el manejo de los números grandes, la funcionalidad de cada una se describe a continuación.

V-A. *Descripción técnica*

La aplicación de minería permite conectarse al servidor, solicitar una transacción de la cola para la determinación de un picadillo que tenga un valor mayor en 10,000 que el valor anterior. Se usó este valor, porque en las pruebas realizadas con dos o tres mineros se necesitaban más de 24 horas para la determinación de un valor válido de nuevo bloque de la *blockchain* según Fig. 1. Los mineros no necesitan autenticación, solo identificarse con una cartera electrónica válida para conectarse al servidor. Los "centicoin" ganados serán acumulados en las correspondientes carteras electrónicas.

En cuanto a la web, los servicios ofrecidos son los siguientes:

- Crear usuarios.
- Un usuario puede crear diferentes direcciones.
- Un usuario puede enviar monedas a otros usuarios mediante su dirección pública.
- Un usuario puede vender monedas a un precio en concreto.
- Un usuario puede comprar monedas.

Cuadro I
ESPECIFICACIONES TÉCNICAS PARA LA WALLET ELECTRÓNICA

Algoritmo de firma	Elliptic Curve Digital Signature Algorithm (ECDSA)
Curva utilizada	Secp256k1
Función Hash para identificador privado	SHA3-256
Función Hash para identificador público	SHA3-256

De acuerdo a los tamaños de llaves y algoritmos sugeridos por el NIST [12][13][14][15] las especificaciones anteriores superan la seguridad mínima requerida en cada uno de ellos siendo como objetivo mínimo una seguridad de 128 bits.

V-B. *Diagrama de funcionamiento*

Cada semilla para generar el nuevo bloque debe asegurar que el hash resultante sea 10000 mayor que el bloque anterior. Encontrar este Hash es el trabajo que deben realizar los mineros

V-C. *Flujo de trabajo*

- Un usuario se registra y se le generan sus identificadores públicos y privados
- Luego de registrado se le asigna una cantidad de 100 sonsocoins
- El usuario puede comenzar a realizar transacciones en la plataforma que funciona como un banco, cada transacción es firmada digitalmente por el emisor
- Los bloques son de 10 transacciones y se confirman cada 5 minutos por los mineros
- Una vez hay transacciones sin confirmar los mineros comienzan a realizar cálculos
- Cuando un bloque es confirmado pasa a formar parte de la base de datos como parte de la *blockchain*.
- Todas las transacciones son consultables desde la plataforma y es posible comerciar con las monedas virtuales

Figura 1. Encontrar el valor válido para el nuevo bloque de la *blockchain*.

V-D. *Implementacíon con Bouncy Castle API*

La API Bouncy Castle cuenta con versiones en C# y Java, la versión en Java permite desarrollo multiplataforma, y entre las primitivas criptográficas ofrecidas están las siguientes: criptografía de llave pública, criptografía de llave privada, funciones hash, códigos de autenticación de mensajes (MAC), firma digital y estampa de tiempo.

Algunos puntos importantes de la librería son: énfasis en el cumplimiento de estándares y normas, amplia documentación disponible en internet e integración transparente con la librería nativa security de java.

Con respecto a las funciones hash y firmas digitales, primitivas usadas en el proyecto, se destaca lo siguiente:

- Entre las funciones hash esta SHA3, pero requirió hacer adecuaciones debido a que la entrada es de cierto tipo y tamaño, así mismo la salida debe ser codificada de acuerdo a los requerimientos de la aplicación.
- La clase que permite implementar firmas digitales cuenta con distintos algoritmos estándares como DSA y ECDSA, para el proyecto se utilizó el segundo. Entre las curvas disponibles están las señaladas por los estándares NIST y SEC, pero fue necesario escribir una implementación para procesar las entradas y salidas del algoritmo al formato necesario y de la misma forma para el algoritmo de verificación.
- La generación del par de llaves privada-pública fue acondicionada para integrarse con el algoritmo de firma y se utilizó el generador de números aleatorios que viene por defecto, además se codificó su salida.

En general para las implementaciones disponibles se requiere escribir código para acondicionarlo al caso específico de aplicación debido a que las entradas y salidas por defecto esperan cierto tipo y tamaño.

V-E. Emulación minería

Para la emulación de los mineros, se diseñó una aplicación de consola en C# que se puede ejecutar en cualquier PC que abre un hilo (thread) de procesador que se comunica por el puerto 3333 al servidor, consistente en una aplicación que se conecta a la base de datos, que del pool de transacciones pendientes obtiene la más antigua, con la finalidad de calcular un hash tal que al convertirlo en decimal sea 10000 mayor que el bloque anterior, usando una cadena codificada en formato JSON con los valores indicados en la Figura 1.

Es de hacer notar que cuando se ejecutan más mineros que números de hilos soportados por el procesador, el sistema completo se ralentiza.

Cada minero accede al último bloque confirmado de la *blockchain*. Este último bloque se usa como parámetro, junto a los datos de la nueva transacción para el cálculo del siguiente bloque.

VI. Experimentos y resultados

De acuerdo a las herramientas creadas el minero se ejecuta en cualquier computadora, este programa se conecta mediante TCP/IP a la plataforma web que almacena la *blockchain* y notifica la confirmación de bloques tanto a la plataforma como a los demás mineros como se muestra en Figura 2.

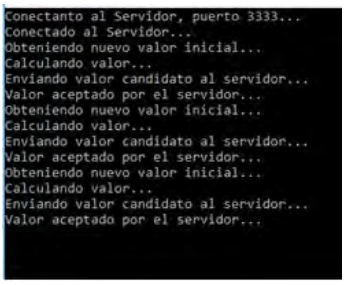


Figura 2. Minero ejecutándose por el puerto 3333.

En la base de datos se generan dos valores según Cuadro III debido a que obtiene la información tanto del que transfiere las monedas como del que las recibe.

Cuadro II
Tabla de transacciones

ID	*Dirección*	*Monto*
1	98db6b79acb71383b5a83e0bbc1cadd4	20
2	d94d81a75c0e8c0aef4e46a08206426b	20

También se cuenta con una ventana donde podemos vender las monedas. Vamos a la pestaña de Venta y seleccionamos nuestra dirección, la cantidad de monedas puestas a la venta y el precio por el cual queremos venderlas.

VII. Conclusiones

- Utilizar la API Bouncy Castle, dada su implementación a bajo nivel para manejo eficiente de los algoritmos criptográficos, requiere más líneas programación y por ende más tiempo, pero permite una mayor personalización de los procesos involucrados en una cadena de bloques, cuestión que en otras librerías como Ethereum o Hiperledge por su alto nivel de abstracción oculta más detalles de la implementación.
- La cadena de bloques propuesta proporciona un ejemplo de la implementación de una criptomoneda dónde se pueden apreciar las ventajas que la tecnología ofrece como la invariación en el tiempo, anonimato, la independencia de un ente central de confianza, por lo anterior las herramientas y código desarrollado pueden servir como base aplicable a futuras implementaciones, dado que no tiene dependencias de bibliotecas externas además de Bouncy Castle.
- En las pruebas realizadas se tuvo que calibrar los tiempos y cantidad de mineros necesarios según la capacidad del procesador y memoria disponible para encontrar los valores óptimos de funcionamiento de la cadena de bloques, comprobando que los recursos de cómputo disponibles y su optimización inciden en la implementación de la minería y rendimiento de la propuesta.

VIII. Recomendaciones

- Se recomienda que en un futuro proyecto se implemente un mecanismo para configurar carteras electrónicas descentralizadas.
- Implementar un mecanismo de consenso para evitar el doble gasto, desafío que se vuelve más difícil con carteras electrónicas descentralizadas.

Agradecimientos

Los autores agradecen enormemente a la universidad de Sonsonate y al Ministerio de la Defensa Nacional, por propiciar la investigación en temas de seguridad informática y especial agradecimiento a la Doctora Lil María Rodríguez Henríquez por su apoyo y asesoría en la investigación.

Referencias

[1] M. Iansiti, K. Lakhani, "The Truth About Blockchain", Harvard Business Review, 2017.
[2] CBInsights Research Portal, "Banking Is Only The Beginning: 42 Big Industries Blockchain Could Transform"[online], disponible en: https://www.cbinsights.com/research/industries-disrupted-blockchain/.
[3] Reuters, Banks adopting blockchain 'dramatically faster' than expected: IBM [online], disponible en: https://www.reuters.com/article/us-tech-blockchain-ibm-idUSKCN11Y28.
[4] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
[5] S. Nakamoto, Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer [online], disponible en: https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf.
[6] A. Narayanan, J. Boneau, E. Felten, A. Miller y S. Goldfeder, Bitcoin and Cryptocurrency Technologies, Princeton: Princeton University Press, 2016.
[7] A. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, CA: O'Reilly, 2014.
[8] The Linux Foundation, Hyperledger [online], 2015, disponible en https://www.hyperledger.org/.
[9] Ethereum Foundation, Ethereum blockchain app platform [online], 2016, disponible en https://www.ethereum.org/.
[10] Legion of the Bouncy Castle, The Bouncy Castle Crypto API [online], 2015, disponible en https://www.bouncycastle.org/.

[11] Scrum Manager Body of Knowledge [online], 2018, disponible en: http://www.scrummanager.net/bok/index.php?title=Scrum_Manager_BoK.
[12] NIST, Digital Signature Standard (DSS) [online], disponible en: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.186-4.pdf.
[13] NIST, Secure Hash Standars (SHS) [online], disponible en: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
[14] Copia de fuentes de las aplicaciones web y de escritorio se encuentra en: http://sonsocoin.mil.sv/content/dist.zip.
[15] NIST, Recommendation for key management [online], disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

Blockchain y control de acceso en la Industria 5.0: Una revisión de los desafíos y oportunidades

R.A.Ibarra-García
CINVESTAV Unidad Guadalajara
Zapopan 45019, México
ricardo.ibarra@cinvestav.mx

A.Díaz-Pérez
CINVESTAV Unidad Guadalajara
Zapopan 45019, México
adiaz@cinvestav.mx

J.L.González-Compeán
CINVESTAV Unidad Tamaulipas
Ciudad Victoria 87130, México
joseluis.gonzalez@cinvestav.mx

***Resumen*—Blockchain ha surgido como una solución emergente para mejorar la transparencia y la descentralización en los sistemas de control de acceso dentro del contexto de la Industria 5.0, caracterizada por entornos interconectados y sistemas ciberfísicos. Sin embargo, a pesar de sus ventajas evidentes, como la mejora de la trazabilidad y la inmutabilidad de los registros, su adopción enfrenta desafíos considerables tales como problemas de escalabilidad y elevados costos computacionales, los cuales dificultan su implementación a gran escala. Este artículo realiza una revisión de la literatura actual, comparando distintos enfoques como el uso de contratos inteligentes, sistemas distribuidos y soluciones híbridas que integran blockchain con tecnologías tradicionales de control de acceso. Además, se exploran los desafíos pendientes y las oportunidades para el desarrollo de sistemas de control de acceso dinámicos y eficientes. Esta revisión proporciona una visión integral del estado de la investigación en blockchain aplicado al control de acceso, destacando su potencial para fortalecer la ciberseguridad en la Industria 5.0 y proponiendo direcciones futuras para investigación y desarrollo.**

***Palabras clave*—blockchain, control de acceso, industria 5.0, ciberseguridad, sistemas ciberfísicos**

I. Introducción

La Industria 5.0 se caracteriza por una convergencia acelerada de tecnologías avanzadas como los sistemas ciberfísicos, el Internet de las Cosas (IoT), la inteligencia artificial (IA) y la conectividad a gran escala [1]. En este contexto, el control de acceso a los sistemas y datos juega un papel fundamental para garantizar la seguridad y la integridad de los procesos industriales y de los flujos de información [2]. Sin embargo, los métodos tradicionales de control de acceso centralizados presentan limitaciones significativas en términos de escalabilidad, transparencia y resiliencia ante ataques. A medida que el número de usuarios y dispositivos crece, estos sistemas enfrentan problemas de rendimiento debido a la concentración de control en una única autoridad central. Además, la falta de transparencia dificulta la auditoría y el monitoreo efectivo de los accesos, lo que puede generar riesgos de seguridad. Por último, la centralización los hace vulnerables a fallos o ataques dirigidos, ya que un único punto de fallo puede comprometer el acceso a todo el sistema [3], [4].

Blockchain se ha convertido en una solución eficaz para mitigar los problemas de centralización y falta de transparencia en los sistemas de control de acceso. Concretamente, la blockchain ofrece ventajas en estos escenarios, tales como [4]–[6]:

- **Descentralización:** Elimina la necesidad de un intermediario central, reduciendo los puntos únicos de fallo y aumentando la confiabilidad del sistema.
- **Inmutabilidad:** Los registros almacenados en la blockchain no pueden ser modificados o alterados, lo que garantiza la integridad de los datos.
- **Transparencia:** Todas las acciones relacionadas con el control de acceso son visibles y verificables, lo que permite auditorías precisas.

A pesar de estas ventajas, la implementación de blockchain en sistemas de control de acceso no está exenta de desafíos. Entre los más significativos se encuentran [7], [8]:

- **Escalabilidad:** Los sistemas basados en blockchain aún enfrentan dificultades para manejar grandes volúmenes de transacciones en tiempo real, lo que puede limitar su aplicabilidad en entornos industriales a gran escala.
- **Costos computacionales:** El mantenimiento de una red blockchain puede implicar altos costos en términos de recursos computacionales y energéticos.

En este artículo, se presenta una revisión de las propuestas más relevantes en la literatura para la integración de blockchain en sistemas de control de acceso, haciendo énfasis en:

- El uso de *contratos inteligentes* para la gestión dinámica de permisos y autorizaciones.
- Sistemas de *control de acceso distribuidos*, que aprovechan las ventajas de la blockchain para mejorar la seguridad y la resiliencia.
- Soluciones *híbridas*, que combinan la blockchain con tecnologías tradicionales para abordar sus limitaciones inherentes.

Además, se identifican los principales desafíos que aún deben resolverse para lograr una implementación exitosa en la Industria 5.0, así como las oportunidades futuras para la investigación y el desarrollo en este campo. Este análisis busca ofrecer una visión integral del estado del arte y proporcionar un punto de partida para futuros estudios sobre el control de acceso en entornos industriales avanzados.

II. Blockchain y control de acceso: Preliminares

En esta sección se introducen los conceptos fundamentales que forman la base de la integración de blockchain con los sistemas de control de acceso, con un enfoque en los modelos más relevantes de control de acceso en la industria actual. Estos conceptos son clave para comprender el desarrollo de propuestas que buscan mejorar la seguridad y eficiencia de los sistemas en la Industria 5.0.

A. Blockchain: Principios fundamentales

Blockchain es una arquitectura compuesta de diversas tecnologías que, en conjunto, permiten su funcionamiento descentralizado, seguro e inmutable, lo cual permite hacer registros que almacenan transacciones en bloques encadenados cronológicamente, garantizando la integridad y seguridad de los datos sin necesidad de una autoridad central. En un entorno de blockchain, cada nodo de la red mantiene una copia del libro mayor, lo que elimina el riesgo de un punto único de fallo y aumenta la resistencia contra ataques externos [9], [10].

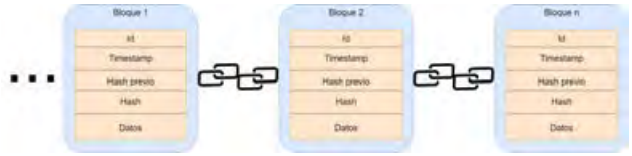


Fig. 1. Representación de una blockchain.

La Figura 1 representa la estructura simplificada de una blockchain. Esta se organiza como una secuencia de bloques enlazados, donde cada bloque contiene los siguientes elementos que aseguran la integridad, seguridad y cronología de los datos:

- **Id**: Es un identificador único del bloque, que lo distingue de otros bloques dentro de la cadena. Generalmente está relacionado con el número de bloque en la secuencia.
- **Timestamp**: Esta es la marca de tiempo que registra el momento exacto en que el bloque fue creado o validado. Es importante para mantener el orden cronológico entre los bloques.
- **Hash previo**: Este campo contiene el hash criptográfico del bloque anterior en la cadena. Es lo que enlaza cada bloque con el anterior, formando una cadena inmutable. Si algún bloque previo es alterado, el hash previo en el bloque siguiente cambiaría, rompiendo la cadena y permitiendo detectar cualquier intento de manipulación.
- **Hash**: Es el hash generado para el bloque actual, calculado a partir de toda la información contenida en el bloque, incluidos los datos. Cualquier alteración en los datos del bloque cambiaría este valor, asegurando así la inmutabilidad de la información.
- **Datos**: Esta sección contiene la información que se quiere almacenar en el bloque. Puede ser información transaccional, contratos inteligentes o cualquier dato que se desee registrar de manera segura y transparente.

Cada bloque está enlazado con el anterior mediante el *hash previo*, lo que garantiza que la cadena sea inmutable y segura. Si un bloque es alterado, todos los bloques siguientes se verán afectados, haciendo evidente cualquier intento de manipulación. La combinación del *hash* y el *hash previo* asegura la integridad y la seguridad de los datos en una blockchain, mientras que el *timestamp* garantiza la secuencia temporal correcta de los eventos.

El consenso entre los nodos se logra a través de diferentes mecanismos (como *Proof-of-Work* o *Proof-of-Stake* [11]) que aseguran que las transacciones sean verificadas y validadas de manera descentralizada. Esta arquitectura ofrece ventajas como la descentralización, transparencia e inmutabilidad [5], [7] que son fundamentales en la implementación de sistemas de control de acceso.

B. Contratos inteligentes

Los contratos inteligentes, o *smart contracts*, son programas informáticos que se ejecutan automáticamente cuando se cumplen condiciones predefinidas. Estos contratos se almacenan en la blockchain y permiten que las partes involucradas en una transacción realicen acuerdos sin necesidad de intermediarios. Una vez que se activan las condiciones establecidas, el contrato inteligente se ejecuta por sí solo, de manera transparente, irreversible y segura [12].

En el contexto del control de acceso, los contratos inteligentes permiten ejecutar reglas de acceso de forma automática, eliminando la necesidad de intervención manual. Esto reduce el tiempo de espera en las decisiones de autorización, lo que mejora el rendimiento en entornos dinámicos como la Industria 5.0, garantizando que solo los usuarios con los derechos apropiados accedan a los recursos correspondientes. Además, al estar registrado en la blockchain, cada ejecución de un contrato inteligente queda almacenada de forma inmutable, lo que facilita las auditorías y el seguimiento de eventos de acceso.

C. Control de acceso: Modelos y tipologías

El control de acceso es un mecanismo importante en los sistemas de seguridad informática para regular qué entidades pueden acceder a qué recursos dentro de un sistema. Existen varios modelos que determinan cómo se gestiona el acceso, dependiendo de las políticas y estructuras organizacionales.

La Figura 2 representa una estructura simplificada de un **sistema de control de acceso a recursos**. En este sistema, múltiples usuarios intentan acceder a un conjunto de recursos protegidos, y su capacidad para hacerlo depende de los permisos y las credenciales que posean. Los componentes principales se describen a continuación:

- **Usuarios (Usuario 1, Usuario 2, Usuario n)**: Cada usuario tiene una llave que simboliza sus credenciales o permisos de acceso. Solo podrán acceder a los recursos si sus credenciales son válidas y coinciden con los requisitos de seguridad del sistema.
- **Llaves de acceso**: Las llaves representan los mecanismos de autenticación que cada usuario debe proporcionar para

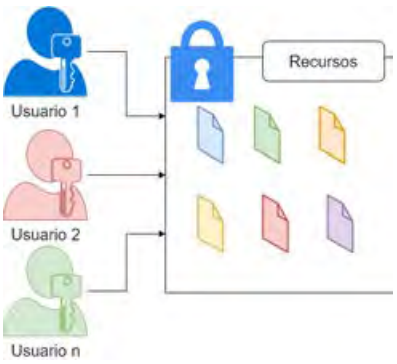


Fig. 2. Representación del control de acceso a recursos.

acceder a los recursos. Estos mecanismos pueden incluir contraseñas, atributos, tokens de seguridad, o certificados digitales que garanticen la autenticidad del usuario.

- **Recursos**: Los recursos, representados por archivos de diferentes colores, simbolizan los activos o datos a los que los usuarios desean acceder. Estos pueden incluir archivos, datos sensibles o servicios a los que se accede de manera controlada.
- **Cerradura y control de acceso**: El ícono de un candado representa el sistema de control de acceso que protege los recursos. Este sistema garantiza que solo los usuarios con las credenciales correctas puedan acceder a los recursos, bloqueando el acceso a quienes no tienen los permisos necesarios.

En resumen, el sistema de control de acceso descrito en la figura asegura que solo los usuarios autorizados puedan acceder a los recursos específicos para los cuales han sido previamente autorizados, mejorando la seguridad y la gestión de la información en entornos controlados.

1) Control de acceso basado en roles: El modelo de *Control de acceso basado en roles* (RBAC) asigna permisos a los usuarios en función de sus roles dentro de una organización. Cada rol tiene un conjunto específico de permisos que le otorgan acceso a ciertos recursos o funciones dentro del sistema. Este enfoque es ampliamente utilizado debido a su simplicidad y facilidad de administración en entornos grandes [13]. Sin embargo, su rigidez puede limitar su aplicabilidad en entornos dinámicos y distribuidos, como la Industria 5.0.

2) Control de acceso basado en atributos: El *Control de acceso basado en atributos* (ABAC) introduce mayor flexibilidad al definir permisos en función de los atributos del usuario, del recurso al que se desea acceder y del contexto. Los atributos pueden incluir propiedades como la ubicación, la hora del día, o el nivel de seguridad requerido. Este enfoque permite una toma de decisiones más dinámica y granular, ideal para entornos altamente interconectados y ciberfísicos [14]. ABAC es particularmente útil en sistemas complejos donde las políticas de acceso requieren ser ajustadas frecuentemente.

3) Control de acceso basado en políticas: El *Ciphertext-Policy Attribute-Based Encryption* (CP-ABE) es un modelo de control de acceso que combina técnicas de cifrado con políticas basadas en atributos para asegurar el acceso a los datos. En este esquema, los datos están cifrados bajo una política que especifica qué atributos debe tener un usuario para poder descifrar la información. CP-ABE es particularmente útil en escenarios donde la confidencialidad de los datos debe ser garantizada incluso cuando se comparten a través de una red abierta [15].

D. Integración de blockchain con control de acceso

La integración de blockchain en los sistemas de control de acceso busca aprovechar las ventajas de la descentralización y la seguridad inherentes a la blockchain para mejorar la eficiencia y fiabilidad de estos sistemas. A continuación, se describen los enfoques más comunes para esta integración:

1) Soluciones distribuidas: La descentralización ofrecida por blockchain permite la creación de soluciones distribuidas para el control de acceso, donde múltiples nodos participan en la toma de decisiones sobre los permisos de acceso. Esto elimina los riesgos asociados a los sistemas centralizados, como los puntos únicos de fallo, y mejora la resiliencia general del sistema [16]. En entornos industriales, estas soluciones distribuidas pueden ser vitales para garantizar el acceso seguro a los datos y sistemas críticos.

2) Sistemas híbridos: Algunas propuestas combinan la blockchain con sistemas de control de acceso tradicionales para crear soluciones híbridas. Estos sistemas utilizan blockchain para gestionar la verificación de identidades y almacenar los registros de acceso de manera inmutable, mientras que los sistemas tradicionales se encargan de la autenticación y autorización en tiempo real [17]. Este enfoque permite aprovechar los beneficios de la blockchain sin incurrir en los costos computacionales que implican algunas soluciones puramente basadas en blockchain.

III. Revisión de literatura

En esta sección, se presentan cinco trabajos recientes que investigan la integración de blockchain con sistemas de control de acceso en diferentes aplicaciones y sectores (ver Tabla I). A continuación se ofrece un resumen de las contribuciones y limitaciones de cada uno de estos estudios.

Priyanka Kamboj, Shivang Khare y Sujata Pal [18] proponen un modelo RBAC que utiliza contratos inteligentes en la plataforma de blockchain Ethereum. La contribución principal es el uso de blockchain para gestionar de forma segura las comunicaciones y autorizaciones de usuarios, eliminando la necesidad de una autoridad centralizada. El modelo propuesto resiste ataques como *man-in-the-middle*, lo que mejora la seguridad en escenarios organizacionales. Además, se probaron las funcionalidades en la red de prueba de Ethereum (Ropsten) para evaluar el costo, la verificación y la autenticación de usuarios.

Contribuciones:

- El uso de **contratos inteligentes** para gestionar permisos de usuario basados en roles, eliminando la dependencia de una autoridad central.

TABLA I
ANÁLISIS CUALITATIVO DE ARTÍCULOS SELECCIONADOS.

Artículo	Enfoque Principal	Ventajas	Desafíos	Experimentación
Kamboj et al. [18]	Autenticación de usuarios usando contratos inteligentes basados en roles	Automatización del control de acceso, mayor seguridad, sin intermediarios	Afectado por escalabilidad y costo de transacciones	Pruebas en Ethereum, evaluando tiempos de autenticación y costos de transacción
Pancari et al. [19]	Comparación de Ethereum y Hyperledger para acceso basado en atributos en IoT	Evaluación de seguridad y rendimiento entre ambas plataformas	La elección práctica depende del entorno	Simulaciones comparativas de latencia y consumo de gas; Hyperledger tuvo mejor rendimiento en redes privadas
Mishra et al. [20]	Compartición de datos médicos con blockchain y CP-ABE optimizado	Mejor rendimiento en cifrado, menor sobrecarga y tiempos de procesamiento	Ataques de retroceso y protección de datos aún son retos	Pruebas de rendimiento en cifrado y tiempos de procesamiento, con mejoras significativas
Banerjee et al. [21]	Control de acceso con CP-ABE multi-autoridad y blockchain en IIoT	Control granular, mayor seguridad y trazabilidad	Sobrecarga computacional y complejidad en gestión distribuida	Evaluación en red privada con mejoras en trazabilidad y seguridad, pero mayor sobrecarga computacional
Wang et al. [22]	Mejora en control de acceso en SWIM con CP-ABE, nube y blockchain	Acceso seguro con soporte a usuarios ligeros	Capacidad computacional limitada en dispositivos ligeros	Simulaciones en dispositivos ligeros, tiempos de procesamiento aceptables con limitaciones en dispositivos de baja capacidad

- Implementación y evaluación del modelo en un entorno real utilizando la red de prueba Ethereum, demostrando su viabilidad.
- La propuesta mejora la **seguridad** al resistir ataques de intermediarios y facilitar la verificación automática de autenticación.

El trabajo de Stefan Pancari *et al.* [19] compara dos plataformas blockchain populares, Ethereum y Hyperledger Fabric, en el contexto de control de acceso basado en atributos (ABAC) para entornos IoT de hogares inteligentes. La comparación se realiza mediante la implementación de contratos inteligentes específicos para ABAC en ambas plataformas y su evaluación bajo diferentes criterios, como seguridad, rendimiento y escalabilidad.

Contribuciones:

- Propuesta de un contrato inteligente original para Ethereum y modificación de un contrato preexistente en Hyperledger Fabric para controlar el acceso en redes IoT domésticas.
- Evaluación de las ventajas y limitaciones de ambas plataformas en cuanto a su capacidad para gestionar el acceso de manera eficiente y segura.

Anil Kumar Mishra y Yogomaya Mohapatra [20] presentan un sistema híbrido de compartición de datos médicos basado en blockchain y cifrado de políticas de atributos (CP-ABE). La propuesta aborda problemas de seguridad comunes en los registros médicos personales (PHR), como el acceso no autorizado y la manipulación de datos. El sistema utiliza blockchain para garantizar la integridad y trazabilidad de los datos, mientras que los contratos inteligentes facilitan el control de acceso y la búsqueda segura en los registros cifrados.

Contribuciones:

- Propuesta de un esquema descentralizado para compartir datos médicos basado en blockchain y CP-ABE, que mejora la privacidad y la eficiencia.
- Implementación de un mecanismo de auditoría de datos y verificación mediante blockchain, garantizando la integridad de los registros.
- Uso de almacenamiento híbrido on-chain/off-chain para reducir los problemas de escalabilidad de la blockchain.

Soumya Banerjee *et al.* [21] presenta un esquema de control de acceso basado en blockchain y en el cifrado basado en políticas de atributos (CP-ABE) en entornos de IIoT. La propuesta aborda el problema de los puntos únicos de fallo que suelen aparecer en sistemas con una única autoridad de control de atributos, utilizando múltiples autoridades para gestionar los atributos. Además, el uso de una blockchain de permisos (Hyperledger Fabric) proporciona un medio seguro y auditable para gestionar los accesos y garantizar la integridad de los registros.

Contribuciones:

- Implementación de un esquema multi-autoridad para gestionar atributos y mitigar problemas de confianza centralizada.
- Uso de contratos inteligentes para reducir la carga de comunicación y cómputo en los usuarios durante el acceso a los datos.

Qing Wang *et al.* [22] presenta un esquema de control de acceso basado en el cifrado de políticas de atributos (CP-ABE) y la fusión de blockchain y computación en la nube para el SWIM (System Wide Information Management). La solución aborda los problemas de seguridad en el intercambio de información dentro del sistema de gestión del tráfico aéreo (ATM). Se proponen algunas mejoras, como el uso de múltiples autoridades para evitar la dependencia de una sola autoridad central, y se emplea blockchain para auditar y registrar el acceso a los datos, lo que garantiza la inmutabilidad de los registros.

Contribuciones:

- Introducción de un esquema multi-autoridad basado en CP-ABE que garantiza un control de acceso distribuido

y seguro en el entorno SWIM.
- Uso de blockchain para registrar de manera auditable las solicitudes de acceso, mejorando la supervisión y la seguridad.
- Implementación de computación subcontratada para reducir la carga computacional en dispositivos con recursos limitados.

IV. Análisis y comparación

Para visualizar la comparación entre los cinco artículos seleccionados, se ha generado un diagrama de radar que evalúa los siguientes criterios: seguridad, escalabilidad, privacidad, eficiencia computacional y latencia. Cada artículo tiene una línea única en el gráfico que refleja su rendimiento en cada una de estas áreas, en una escala del 1 al 5, donde 5 es la mejor puntuación.

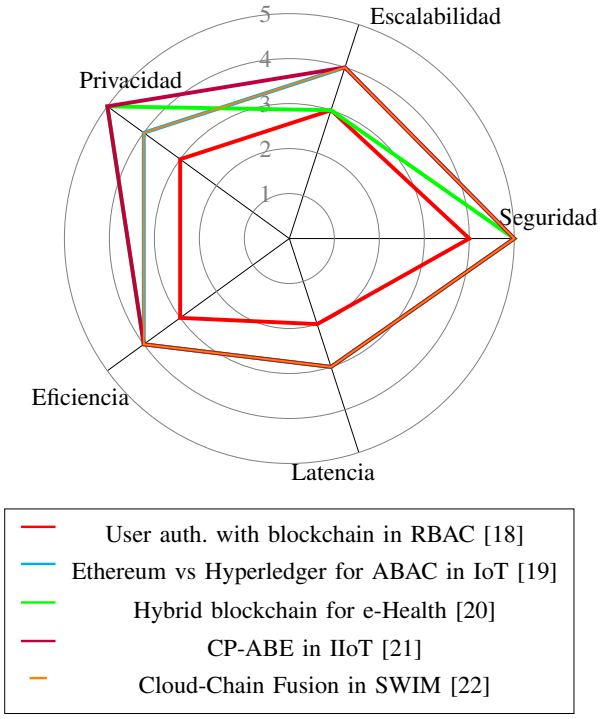


Fig. 3. Comparación de los artículos en términos de Seguridad, Escalabilidad, Privacidad, Eficiencia y Latencia.

La Figura 3 muestra una comparación clara entre cinco artículos en términos de seguridad, escalabilidad, privacidad, eficiencia y latencia. Ethereum vs Hyperledger for ABAC in IoT y CP-ABE in IIoT sobresalen en seguridad con puntuaciones máximas de 5, destacando su enfoque robusto en protección de datos, mientras que Hybrid blockchain for e-Health es líder en privacidad, garantizando una alta protección de datos personales. User auth. with blockchain in RBAC tiene puntuaciones moderadas en escalabilidad y eficiencia, pero su latencia es la más baja, lo que sugiere problemas de rendimiento en tiempo real. Por otro lado, Cloud-Chain Fusion in SWIM y CP-ABE in IIoT son soluciones equilibradas con buenas puntuaciones en todas las categorías, lo que indica que son opciones versátiles y bien balanceadas para su implementación.

V. Desafíos y oportunidades futuras en la Industria 5.0

La Industria 5.0 representa un cambio de paradigma que va más allá de la automatización y digitalización de los procesos industriales que caracterizaban a la Industria 4.0. En esta nueva era, se busca una mayor integración entre los seres humanos y las máquinas, con un enfoque en la personalización y la sostenibilidad [23]. En este contexto, blockchain y el cifrado basado en atributos (CP-ABE) juegan un papel fundamental para garantizar la seguridad, la privacidad y la escalabilidad en los sistemas de control de acceso.

A. Desafíos actuales en la integración de blockchain con sistemas de control de acceso

La integración de blockchain con esquemas de control de acceso basados en atributos, como CP-ABE, enfrenta una serie de desafíos técnicos que deben ser abordados para su adopción generalizada en la Industria 5.0. Algunos de los principales desafíos incluyen:

- **Escalabilidad**: Aunque blockchain ofrece una solución descentralizada y segura para el control de acceso, su rendimiento puede verse comprometido en aplicaciones a gran escala debido a las limitaciones inherentes en la capacidad de procesamiento y el consumo de recursos computacionales. La integración con CP-ABE también aumenta la complejidad debido al procesamiento de claves y atributos.
- **Latencia**: El tiempo necesario para verificar y autorizar las solicitudes de acceso en un entorno basado en blockchain puede ser un problema crítico en la Industria 5.0, donde la inmediatez de las decisiones es clave. La combinación de blockchain con CP-ABE introduce una capa adicional de complejidad que podría incrementar la latencia en el proceso de acceso.
- **Privacidad**: Aunque CP-ABE es eficaz para garantizar la privacidad en los sistemas de control de acceso, la combinación con blockchain podría comprometerla debido a la naturaleza pública de algunas cadenas de bloques. Se requiere una investigación adicional para desarrollar mecanismos que garanticen que los datos cifrados sigan siendo privados en una infraestructura.

B. Oportunidades futuras hacia la Industria 5.0

A pesar de los desafíos mencionados, la integración de blockchain y CP-ABE ofrece oportunidades prometedoras para la evolución de la Industria 5.0. Entre las principales oportunidades destacan:

- **Sistemas de control de acceso descentralizados**: La Industria 5.0 necesitará sistemas más resilientes y adaptativos. La combinación de blockchain y CP-ABE proporciona una infraestructura robusta para gestionar el acceso

a recursos distribuidos en tiempo real, eliminando los riesgos asociados con los puntos únicos de fallo.

- **Privacidad y seguridad mejoradas**: La capacidad de blockchain para garantizar la inmutabilidad y la trazabilidad de los datos, junto con la flexibilidad de CP-ABE para gestionar permisos dinámicos basados en atributos, crea un marco sólido para la protección de la información sensible en entornos industriales interconectados.
- **Automatización inteligente**: Los contratos inteligentes integrados en blockchain permiten la automatización de procesos de control de acceso de manera segura y eficiente. Esto, combinado con el cifrado basado en atributos, permite una gestión del acceso altamente personalizable y adaptada a las necesidades individuales de los usuarios en la Industria 5.0.

En resumen, aunque la integración de blockchain y CP-ABE en la Industria 5.0 enfrenta desafíos significativos, sus ventajas en términos de seguridad, privacidad y automatización presentan una gran oportunidad para el futuro de los sistemas industriales. La investigación y el desarrollo continuarán avanzando para optimizar estas tecnologías y garantizar su adopción en los próximos años.

VI. Conclusiones

La integración de blockchain y el control de acceso presenta un enfoque prometedor para abordar los desafíos de seguridad, privacidad y escalabilidad en la Industria 5.0. A lo largo del artículo, se ha discutido cómo blockchain puede garantizar la inmutabilidad y trazabilidad de los datos, mientras que soluciones como CP-ABE ofrecen flexibilidad en la gestión de permisos dinámicos. Sin embargo, persisten desafíos relacionados con la escalabilidad y la latencia que deben resolverse para su adopción en entornos industriales a gran escala.

A pesar de estas limitaciones, las oportunidades que brindan estas tecnologías, como la creación de sistemas de control de acceso descentralizados y la mejora de la privacidad, son significativas. La Industria 5.0 requerirá sistemas más resilientes, automatizados y personalizados, y la combinación de blockchain con CP-ABE ofrece una vía clara para cumplir con estas expectativas.

En conclusión, la continua investigación y desarrollo en la integración de estas tecnologías permitirá optimizar sus capacidades y contribuir a la evolución de entornos industriales seguros y eficientes en la era de la Industria 5.0.

Referencias

[1] J. Leng, W. Sha, B. Wang, P. Zheng, C. Zhuang, Q. Liu, T. Wuest, D. Mourtzis, and L. Wang, "Industry 5.0: Prospect and retrospect," *Journal of Manufacturing Systems*, vol. 65, p. 279–295, October 2022.

[2] B. Leander, A. Causevic, T. Lindstrom, and H. Hansson, "A questionnaire study on the use of access control in industrial systems," in *2021 26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, vol. 2020 june, p. 1–8, IEEE, September 2021.

[3] D. Wu, X. Huang, X. Xie, X. Nie, L. Bao, and Z. Qin, "Ledge: Leveraging edge computing for resilient access management of mobile iot," *IEEE Transactions on Mobile Computing*, vol. 20, p. 1110–1125, March 2021.

[4] J. Zarrin, H. Wen Phang, L. Babu Saheer, and B. Zarrin, "Blockchain for decentralization of internet: prospects, trends, and challenges," *Cluster Computing*, vol. 24, p. 2841–2866, May 2021.

[5] R. Saha, G. Kumar, M. Conti, T. Devgun, T.-h. Kim, M. Alazab, and R. Thomas, "Dhacs: Smart contract-based decentralized hybrid access control for industrial internet-of-things," *IEEE Transactions on Industrial Informatics*, vol. 18, p. 3452–3461, May 2022.

[6] J. Sedlmeir, J. Lautenschlager, G. Fridgen, and N. Urbach, "the transparency challenge of blockchain in organizations," *Electronic Markets*, vol. 32, p. 1779–1794, March 2022.

[7] A. Aldoubaee, N. H. Hassan, and F. A. Rahim, "A systematic review on blockchain scalability," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 9, 2023.

[8] M. Oliveira, S. Chauhan, F. Pereira, C. Felgueiras, and D. Carvalho, "Blockchain protocols and edge computing targeting industry 5.0 needs," *Sensors*, vol. 23, p. 9174, Nov. 2023.

[9] N. Ul Hassan, C. Yuen, and D. Niyato, "Blockchain technologies for smart energy systems: Fundamentals, challenges, and solutions," *IEEE Industrial Electronics Magazine*, vol. 13, p. 106–118, December 2019.

[10] R. K. Raman and L. R. Varshney, "Coding for scalable blockchains via dynamic distributed storage," *IEEE/ACM Transactions on Networking*, vol. 29, p. 2588–2601, December 2021.

[11] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, IEEE, October 2017.

[12] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," *Future Generation Computer Systems*, vol. 105, p. 475–491, April 2020.

[13] J. Xu, Y. Yu, Q. Meng, Q. Wu, and F. Zhou, "Role-based access control model for cloud storage using identity-based cryptosystem," *Mobile Networks and Applications*, vol. 26, p. 1475–1492, January 2020.

[14] L. Karimi, M. Aldairi, J. Joshi, and M. Abdelhakim, "An automatic attribute-based access control policy extraction from access logs," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, p. 2304–2317, July 2022.

[15] P. Sharma, R. Jindal, and M. D. Borah, "Blockchain-based cloud storage system with cp-abe-based access control and revocation process," *The Journal of Supercomputing*, vol. 78, p. 7700–7728, January 2022.

[16] N. Shi, L. Tan, C. Yang, C. He, J. Xu, Y. Lu, and H. Xu, "Bacs: A blockchain-based access control scheme in distributed internet of things," *Peer-to-Peer Networking and Applications*, vol. 14, p. 2585–2599, June 2020.

[17] Z. Cui, F. Xue, S. Zhang, X. Cai, Y. Cao, W. Zhang, and J. Chen, "A hybrid blockchain-based identity authentication scheme for multi-wsn," *IEEE Transactions on Services Computing*, p. 1–1, 2020.

[18] P. Kamboj, S. Khare, and S. Pal, "User authentication using blockchain based smart contract in role-based access control," *Peer-to-Peer Networking and Applications*, vol. 14, p. 2961–2976, April 2021.

[19] S. Pancari, A. Rashid, J. Zheng, S. Patel, Y. Wang, and J. Fu, "A systematic comparison between the ethereum and hyperledger fabric blockchain platforms for attribute-based access control in smart home iot environments," *Sensors*, vol. 23, p. 7046, August 2023.

[20] A. K. Mishra and Y. Mohapatra, "Hybrid blockchain based medical data sharing with the optimized cp-abe for e-health systems," *International Journal of Information Technology*, vol. 16, p. 121–130, December 2023.

[21] S. Banerjee, B. Bera, A. K. Das, S. Chattopadhyay, M. K. Khan, and J. J. Rodrigues, "Private blockchain-envisioned multi-authority cp-abe-based user access control scheme in iiot," *Computer Communications*, vol. 169, p. 99–113, March 2021.

[22] Q. Wang, L. Zhang, X. Lu, and K. Wang, "A multi-authority cp-abe scheme based on cloud-chain fusion for swim," in *2022 IEEE Intl Conf on Parallel; Distributed Processing with Applications, Big Data; Cloud Computing, Sustainable Computing; Communications, Social Computing; Networking (ISPA/BDCloud/SocialCom/SustainCom)*, p. 213–219, IEEE, December 2022.

[23] A. Verma, P. Bhattacharya, N. Madhani, C. Trivedi, B. Bhushan, S. Tanwar, G. Sharma, P. N. Bokoro, and R. Sharma, "Blockchain for industry 5.0: Vision, opportunities, key enablers, and future directions," *IEEE Access*, vol. 10, p. 69160–69199, 2022.

Sistema de cifrado robusto para imágenes digitales basado en autómatas celulares y S-box

Juan José Contreras Torres
Coordinación Académica Región Altiplano Oeste
Universidad Autónoma de S L. P.
Salinas, Mexico
juanjosetorres96@outlook.com

Marco Tulio Ramírez Torres
Coordinación Académica Región Altiplano Oeste
Universidad Autónoma de S L. P.
Salinas, Mexico
tulio.torres@uaslp.mx

Ricardo Eliu Lozoya Ponce
Academia de Ingeniería
Universidad de Guadalajara
Guadalajara, México
rlozoya@academicos.udg.mx

Jesús Agustín Aboytes González
Instituto de Investigación en Comunicación Óptica
Universidad Autónoma de S L. P.
San Luis Potosí, México
agustin.aboytes@upslp.edu.mx

***Abstract*— En esta investigación se presenta la implementación y validación de un sistema de cifrado de imágenes digitales. Este sistema busca proporcionar seguridad criptográfica y perceptual a imágenes que posean una alta redundancia de datos, utilizando cajas de sustitución y autómatas celulares. Las cajas de sustitución son diseñadas bajo diversos criterios con el fin de superar los ataques de criptoanálisis y cumplir con el criterio Avalanche. El problema al usar cajas de sustitución radica cuando el texto plano es altamente redundante, porque la sustitución se realiza siempre por el mismo valor, dejando notar patrones de la imagen original. Por otro lado, la sincronización de autómatas celulares ha demostrado ser sensible a condiciones iniciales al grado que puede usarse para diseñar generadores de números pseudoaleatorios. Por lo tanto en este sistema se combinan ambas técnicas para lograr un sistema seguro y robusto para el cifrado de imágenes.**

Keywords*— *autómatas celulares, cifrado, S-box.

I. INTRODUCCION

Cada vez es más frecuente que podamos realizar más operaciones vía internet, facilitando así los procesos y optimizando tiempos. Sin embargo, esto requiere brindar seguridad a los usuarios, dado que sus datos se encuentran expuestos en las transmisiones o en el lugar de almacenamiento. Una de las técnicas empleadas para proteger información son los algoritmos criptográficos. Esta técnica consiste en volver ininteligible la información, de forma tal que solo pueda ser recuperada utilizando la clave correcta.

En la actualidad el cifrado de imágenes es un campo de investigación muy activo, debido a las múltiples áreas donde se requiere, por ejemplo: en el servicio de televisión de paga, sistemas de imagen médica, videoconferencias, comunicaciones militares, video vigilancia, entre otras. A pesar de que se cuenta con varios algoritmos de cifrado convencionales, como lo son AES (Advanced Encryption Standard), DES (Data Encryption Standard) e IDEA (International Data Encryption Algorithm), han resultado en muchas ocasiones imprácticos para el cifrado de imágenes, debido a las propiedades intrínsecas de éstas, tales como una gran tasa de datos, una fuerte correlación adyacente, una alta redundancia, entre otras [1]. Por lo tanto, el problema de seguridad se extiende debido a que los algoritmos para cifrado de imágenes deben brindar seguridad perceptual y seguridad criptográfica.

Lo anterior ha fomentado la búsqueda e implementación de nuevos esquemas de cifrado de imágenes, como lo son los sistemas de cifrado con enfoque caótico. Es por eso que en esta investigación se conjunta la sincronización de autómatas celulares basada en la regla 90, la cual es de dinámica caótica discreta y las cajas de sustitución (S-box) para brindar un algoritmo fuerte contra ataques de criptoanálisis diferencial y estadísticos. El artículo se compone de la siguiente manera, en el capítulo 2 se describe el marco teórico y el método de cifrado, mientras que en el capítulo 3 se muestran los resultados obtenidos en distintas pruebas de seguridad. El capítulo 4 contienen las conclusiones de la investigación.

II. ANTECEDENTES

A. Autómatas celulares

El concepto de autómata celular (AC) fue introducido en la década de los años 40 por el matemático John von Neumann y Stanislaw Ulam [2]. Los AC son usados para modelar comportamientos complejos donde se involucran interacciones locales. De hecho, los AC representan una clase de sistemas dinámicos capaces de describir la evolución de sistemas utilizando reglas simples, sin la necesidad de utilizar ecuaciones diferenciales.

Los autómatas celulares consisten en un conjunto ordenado de celdas, en forma de rejilla, donde cada celda tiene un número finito de estados. Los autómatas celulares forman una rejilla de dos dimensiones, donde sus celdas evolucionan en pasos discretos acorde a una regla local de actualización aplicada de manera uniforme, sobre todas las celdas. En el inicio, un estado es asignado a las celdas en el tiempo t=0, donde los nuevos estados de la celda dependerán de sus estados previos y los de su vecindad, como se muestra en Fig. 1.

Los autómatas celulares elementales (ACE) son AC de una dimensión, con dos estados y de vecindad de radio 1. Una regla local de autómatas celulares es el algoritmo usado para calcular el siguiente estado de la celda. Los ACE difieren entre sí, solo por la elección de la regla local, contienen solo

tres variables (celdas) y cada una puede tomar solo dos valores (1,0), por lo tanto existen solo 8 combinaciones, resultando 2^8=256 reglas locales y ACE diferentes. Por ejemplo, la regla local 90 es descrita por la siguiente expresión:

$$x_i^{t+1} = \mathcal{A}(x_{i-1}^t + x_{i+1}^t) \quad (1)$$

El fenómeno de sincronización ocurre cuando después de un periodo de tiempo, los comportamientos de dos sistemas dinámicos se aproximan arbitrariamente. En el caso de AC, después de un número de pasos en el tiempo *t*, la diferencia entre los vectores **x** y **y** correspondientes al autómata celular controlador y replica respectivamente, eventualmente resultará el vector nulo **0**= (0,0….0). Para esto es necesario que en cada paso, ambos vectores evolucionen usando la misma regla local.

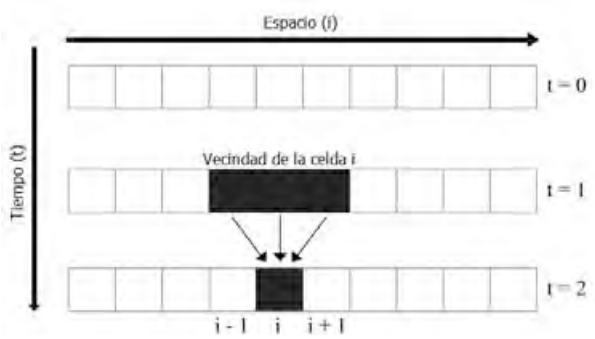


Fig. 1. Diagrama espacio-tiempo de un automata celular

En la referencia [3] se demostró que un par de ACE que evolucionan utilizando la regla local 90, sincronizan si las coordenadas acopladas están separadas por un bloque de N=2^n-1 sitios desacoplados, siendo *n* un entero positivo. Basado en el fenómeno de sincronización, en [4] los autores propusieron un Generador de Números Pseudo-Aleatorios (GNPA). La función principal es llamada *h*, y requiere dos vectores **x** y **y** de *n* bits y *n+1* bits respectivamente. Para calcular una secuencia pseudo-aleatoria, la función requiere que el autómata celular evolucione hacia atrás. Tal situación es descrita en la Fig. 2, donde las compuertas XOR son representadas con los círculos que en medio tienen una cruz, la conectividad de éstas representan la regla local 90, y el vector resultante es llamado vector **t**.

En la referencia [5] se creó una función de preprocesmiento para intercambiar los valores del texto en claro, basada en el generador de números pseudo-aleatorios, haciendo una modificación en su retroalimentación, ver Fig. 3. El proceso aplicado a imágenes consiste en recibir cada coeficiente de pixel como si fuera el vector **x**, el vector **y** sera sustituido después de cada iteración por el vector **m** resultante, concatenando el bit menos significativo del vector **y** precedente como el bit más significativo del nuevo vector. Esta función permite romper la alta correlación adyacente de las imágenes, permitiendo una sustitución dinámica de la información.

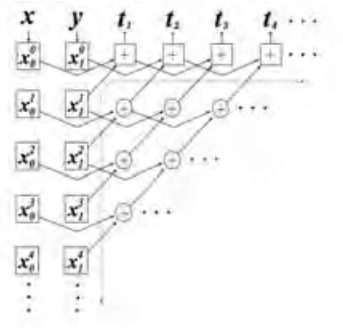


Fig. 2. Generador de secuencias pseudo-aleatorias

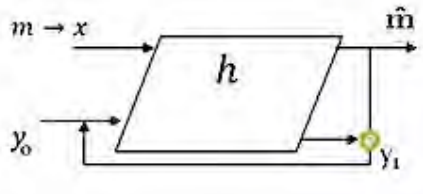


Fig. 3. Función de preprocesamiento basado en la funcin *h*.

B. S-box

Por otra parte, en la criptografía, las cajas de sustitución son un componente básico en los algoritmos simétricos. La cajas son utilizadas en bloques cifradores para intercambiar el texto en claro y de esta manera ocultar la relación entre la llave de cifrado y el texto cifrado [6].

El diseño y selección de una caja de sustitución es un proceso cuidadoso, porque requiere ser resistente a ataques de criptoanálisis. La Fig. 4 muestra la S-box empleada en el sistema de encriptación AES.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	IE	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Fig. 4. Caja de sustitucion del sistema AES en notacion hexadecimal.

Por lo tanto, para el desarrollo de este algoritmo de cifrado de imágenes encontramos viable unir ambas herramientas. La

operación de preprocesamiento es capaz de romper la alta correlación de las imágenes y las cajas de sustitución proveen de seguridad ante ataques de criptoanálisis diferencial y que cumplen con el criterio Avalanche.

Para incrementar la condición inicial se realizó una nueva versión de la operación de preprocesmiento, donde se utilizan tres operaciones *h*. Ver Fig. 5.

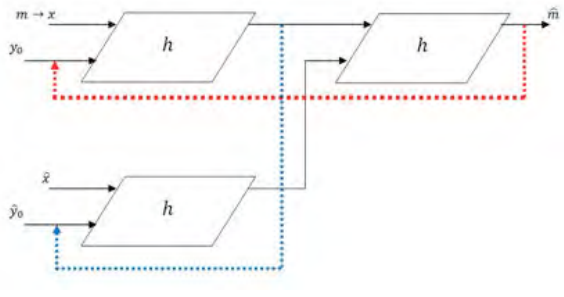


Fig. 5. Función de procesamiento mejorado con tres funciones *h*.

El algoritmo para cifrar una imagen funciona de la siguiente manera:

1º Se toman bloques de texto en claro de 24 bits (3 pixeles en escala de grises)

2º Se aplica el preprocesamiento a todos los bloques de la imagen.

3º Después se sustituye el valor de cada pixel utilizando una S-box

4º Posteriormente se invierten las columnas y los renglones de la imagen resultante de forma tal que el pixel (n,n) ocupe ahora el lugar (0,0).

5º Finalmente se utiliza otra vez la función de preprocesamiento con la imagen transformada.

La llave secreta de este algoritmo es de al menos 148 bits ya que se utilizan dos funciones de preprocesamiento extendidas.

III. RESULTADOS

A continuación se muestran los resultados del análisis de seguridad aplicado a las imágenes cifradas. Se aplicaron diversas pruebas estadísticas, ataques de criptánalisis y el cálculo de los índices NPCR (Number of Changing Pixel Rate) y UACI (Unified Averaged Changed Intensity) para validar los resultados ante ataques de criptoanálisis diferencial.

Para las pruebas, usamos imágenes ampliamente utilizadas en el procesamiento de imágenes con diferente actividad óptica: mandril, Lena y pimientos. Todas en escala de grises a 8 bits y de dimensiones 512 x 512 pixeles. Podemos ver dos de ellas en las Fig. 6a) y 7a).

La primera prueba consiste en el cálculo de histogramas tanto de la imagen en claro como de su versión cifrada. La Fig. 6 muestra el caso de la imagen de Lena, donde podemos ver que el histograma de su versión cifrada es uniforme, ocultando así la redundancia de datos de la imagen original.

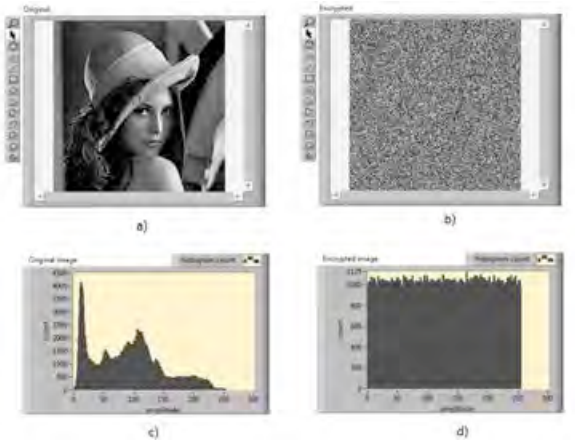


Fig. 6. Análisis de histogramas a) Imagen de Lena, b) Imagen de Lena cifrada, c)Histograma de la imagen original de Lena y d) Histograma de la versión cifrada de Lena.

La segunda prueba que se realizó fue el cálculo del coeficiente de correlación entre las dos imágenes. Esta prueba trata de demostrar la independencia que existe entre la imagen cifrada y la imagen original. Acorde a la interpretación de este valor, sabemos que no existe correlación entre las imágenes si el resultado es próximo a 0. La Tabla 1 muestra los resultados de esta prueba aplicada a las tres imágenes de prueba.

TABLA I. COEFICIENTE DE CORRELACIÓN

Imagen	Coeficiente
Pimientos	-0.0013268
Lena	0.0020740
Mandril	-0.0002453

En el cifrado de imágenes es común analizar la resistencia de los algoritmos ante ataques diferenciales utilizando dos medidas: NPCR y UACI. Ambas mediciones están basadas en pequeños cambios en dos imágenes y cifrarlas bajo la misma llave. Para ilustrar esto, asumamos que tenemos dos imágenes cifradas C^1 y C^2, cuyas imágenes en claro correspondientes tiene solo un pixel diferente entre sí, y ambas han sido cifradas con la misma llave. Los coeficientes en la escala de grises de ambas imágenes en el renglón i y la columna j son señalados como $C^1(i, j)$ y $C^2(i, j)$ respectivamente. Los índices NPCR y UACI son definidos en las ecuaciones (2) y (3).

$$NPCR: N(C^1, C^2) = \sum_{i,j} \frac{D(i,j)}{T} \times 100\% \quad (2)$$

$$UACI: U(C^1, C^2) = \sum_{i,j} \frac{|C^1(i,j) - C^2(i,j)|}{F \cdot T} \times 100\% \quad (3)$$

donde D(i, j) está determinado de la siguiente manera: si $C^1(i, j) = C^2(i, j)$, entonces D(i, j) = 0, de otra manera D(i, j) = 1, T es el total de pixeles de las imágenes y F denota el valor máximo valido en el formato de la imagen. Para imágenes en escala de grises a 256 niveles, los valores teóricos son UACI=33.464% y NPCR=99.609%, ver [7]. Los resultados obtenidos para nuestro algoritmo se muestran en la Tabla II, donde se cambió el bit menos significativo del pixel del reglón y columna 255.

TABLA II. NPCR Y UACI

Imagen	NPCR	UACI
Pimientos	99.6235%	33.434992%
Lena	99.6021%	33.425587%
Mandril	99.6128%	33.361058%

Como se puede observar en la mayoría de las ocasiones se sobrepasan los valores teóricos y en los casos donde son menores, se encuentran dentro del rango de valores críticos, acorde a [7]. Gracias al 4º paso del algoritmo, sin importar que pixel se modifique, el sistema siempre pasa la prueba.

Por último, realizamos el ataque Chosen-plainimage attack (CPIA). En la referencia [8] señalan que si un criptosistema es seguro contra el ataque CPIA, también es seguro contra otros ataques de criptoanálisis tales como cipherimage-only attack o known-plainimage attack. Este ataque implica que el adversario es capaz de escoger las imágenes en claro y obtener su respectiva versión cifrada, pero no conoce la llave secreta. El ataque comienza seleccionando las imágenes a cifrar, como se puede ver en la Fig. 7, se utilizan la imagen de los pimientos, Fig. 7a) y una imagen negra sólida, Fig. 7c). Ambas imágenes son cifradas bajo la misma llave secreta, los resultados son Fig. 7b) y 7d). Por último, se realiza una operación XOR pixel a pixel entre ambas imágenes cifradas, el resultado será lo que se denomina imagen recuperada, Fig. 7e). Como podemos observar en nuestro caso la imagen resultante no revela información de la imagen original.

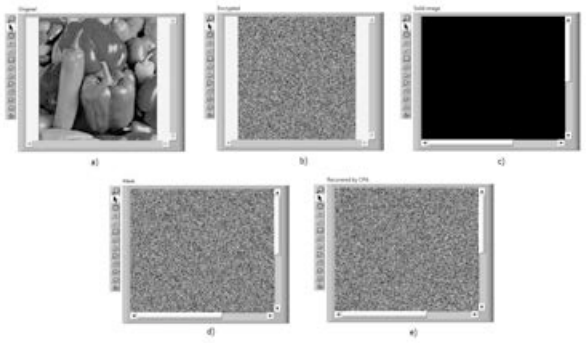


Fig. 7. Chosen-plainimage attack aplicado a la imagen de prueba de los pimientos. a) Imagen original, b) imagen cifrada de los pimientos, c) imagen solida escogida, d) imagen máscara y e) la imagen recuperada.

Para corroborar que no existe relación entre la imagen recuperada y la imagen original calculamos nuevamente el coeficiente de correlación entre ambas imágenes. Los resultados se muestran en la Tabla 3.

TABLA III. COEFICIENTE DE CORRELACIÓN

Imagen	Coeficiente
Pimientos	-0.0064724
Lena	0.0046168
Mandril	0.0081693

IV. CONCLUSIONES

En el presente trabajo se propuso un algoritmo para el cifrado de imágenes que, sin importar el nivel óptico de actividad, fuera capaz de ofrecer seguridad criptográfica y perceptual. Ambas herramientas, la sincronización de autómatas celulares y las cajas de sustitución se complementan para cifrar de manera segura esta información.

Como se puede observar en cada una de las pruebas, el algoritmo propuesto pasó de manera exitosa cada una de ellas. La condición inicial o llave de secreta es de 145 bits, por lo tanto, dado el procesamiento actual no es susceptible a romperse utilizando fuerza bruta [9].

V. AGRADECIMIENTOS

M. T. Ramírez-Torres agradece el apoyo recibido por el Proyecto FAI-UASLP con número de registro C18-FAI-05-55.55. Y al PFCE por el apoyo otorgado a la CARAO en el recurso P/PFCE 2018-24MSU0011E22.

REFERENCIAS

[1] S. Lian. Multimedia content encryption: Techniques and applications. New York: Auerbach Publications, 2009.

[2] J. von Neuman. Theory of Self-Reproducing Automata. Urbana: University of Illinois Press, 1996.

[3] J. Urías, E. Ugalde, G. Salazar, "Synchronization of cellular automaton pairs," Chaos: An Interdisciplinary Journal of Nonlinear Science, vol. 8(4), pp. 814–818, November 1998.

[4] J. Urías, E. Ugalde, G. Salazar, "A cryptosystem based on cellular automata," Chaos: An Interdisciplinary Journal of Nonlinear Science, Vol. 8(4). 819–822, November 1998.

[5] M. T. Ramírez-Torres, J. S. Murguía, M. Carlos Mejía, "Image encryption with an improved cryptosystem based on a matrix approach," IJMP C, vol. 25, no. 10, p. 1450054, April 2014.

[6] J. Chandrasekaran, B. Subramanyan & R. Selvanayagam, "A chaos based approach for improving non linearity in S box design of symmetric key cryptosystems," in International Conference on Computer Science and Information Technology, Bangalore, pp. 516-522, Janaury 2011.

[7] Y. Wu, J. P. Noonan, S. Agaian, "NPCR and UACI randomness tests for image encryption," Cyber journals: multidisciplinary journals in science and technology, JSAT, 2011, vol. 1, no. 2, pp. 31-38, April 2011.

[8] A. M. del Rey, G. R. Sánchez & A. De La Villa Cuenca "Encrypting digital images using cellular automata" in International Conference on Hybrid Artificial Intelligence Systems, Salamanca, pp. 78-88, March 2012.

[9] C. Paar and J. Pelzl. Understanding cryptography: a textbook for students and practitioners. New York: Springer-Verlag, 2010.

Aplicación a la criptografía de sistemas caóticos lineales por pedazos mediante el aumento de puntos de equilibrio

González Del Río Juan Daniel; Ontañón-García Pimentel Luis Javier; Ramírez Torres Marco Tulio,
Coordinación Académica Región Altiplano Oeste, Universidad Autónoma de San Luis Potosí,
Kilómetro 1 Carretera a Santo Domingo, 78600, Salinas de Hidalgo, San Luis Potosí, México,
j.danielgr18@hotmail.com ; luis.ontanon@uaslp.mx ; tulio.torres@uaslp.mx

***Resumen*—En este trabajo de investigación se realizó el estudio y aplicación de sistemas caóticos basados en el uso de sistemas lineales por pedazos, los cuales pueden ser una gran contribución a la encriptación de datos debido a que estos sistemas son fáciles de implementar y además presentan trayectorias caóticas óptimas para los procesos de encriptación. Para esto se utilizó un análisis de la ubicación de los puntos de equilibrio y número de enroscados, con la finalidad de generar un sistema multienroscado. Para el sistema de encriptación se tomó la secuencia dada por el generador como una llave de cifrado y se realizó la unión con los datos de entrada por medio de la operación XOR para producir la encriptación de imágenes en escala de grises. Se efectuó el análisis de seguridad estadístico para determinar la eficiencia del encriptado propuesto y corroborar los datos mediante coeficientes de correlación e histogramas. La cual nos llevará a establecer un sistema de comunicación de video confidencial.**

Palabras clave— Encriptación, cifrado de imágenes, sistemas lineales por pedazos, Caos.

I. Introducción

La idea de transmitir información sensible y ocultarla de manera segura ante posibles intrusos y piratas informáticos, ha generado un impacto muy fuerte en la comunidad científica que inspira a muchos investigadores a combinar una gran variedad de enfoques para abordar este desafiante problema. Varios métodos que enmascaran la información transmitida han sido propuestos durante los últimos años. Estos métodos de encriptación se basan en muchas técnicas diferentes, por ejemplo, encriptación parcial [1], patrones de exploración [2], autómata celular [3,4], entre otros. Una de las áreas que ha comenzado a llamar la atención en la criptografía es el caos. Esto se debe a la dinámica intrínseca de este tipo de sistemas y la relación entre el caos y la criptografía.

Con los crecientes volúmenes de información generada en tiempo real, se necesitan nuevos mecanismos para garantizar la seguridad y evitar el acceso a personas no autorizadas. Los métodos de encriptación convencionales no son apropiados para imágenes, ya que son propensos a ataques estadísticos debido a la fuerte correlación entre píxeles adyacentes y el análisis de histogramas que pueden ayudar a identificarlos dentro de la imagen; con este objetivo en mente, en este trabajo se propone un algoritmo de encriptación mediante el uso de sistemas lineales por pedazos el cual puede llegar a prevenir que una persona no deseada descifre el mensaje encriptado si es que ésta desconoce los parámetros del oscilador usado y las condiciones iniciales del mismo.

En [5], M. García y colaboradores, trabajaron con atractores basados en sistemas lineales por pedazos de diferente número de enroscados, en donde los sistemas y puntos de equilibrio se localizaban únicamente a lo largo del eje x. Por lo tanto, surge la siguiente pregunta: ¿qué pasaría con la secuencia de la llave cifrada si los enroscados no solo crecieran en el eje x, sino también en el eje y? Tomando esto en consideración, en este trabajo de investigación se desarrolla un algoritmo para ubicar puntos de equilibrio en un sistema lineal por pedazos localizados tanto en el eje x como en el eje y, realizando de esta manera un sistema con un mayor número de enroscados que resulte en trayectorias más complejas.

II. Desarrollo

A. Sistemas caóticos.

La construcción de sistemas dinámicos que muestran un comportamiento caótico es relevante en diversas disciplinas científicas. Por ejemplo, la biología y la meteorología. Estos sistemas modelados matemáticamente por ecuaciones diferenciales ordinarias de primer orden no lineales con parámetros adecuados para garantizar comportamientos caóticos generan atractores extraños. Muchos de los fenómenos no lineales observados en la naturaleza o por el hombre han sido descritos por sistemas caóticos debido a la riqueza de sus comportamientos dinámicos: ciclos límite, órbitas y atractores extraños, etc. Y desde hace algunas décadas, la generación de trayectorias caóticas se ha buscado simplificar con respecto a sus ecuaciones o implementaciones electrónicas. Es por esto por lo que los sistemas lineales por pedazos (PWL) han sido de gran utilidad en este tema. Estos sistemas se basan en parámetros de conmutación que se pueden visualizar como un conjunto de subsistemas y una señal de conmutación que los selecciona durante un intervalo determinado de tiempo.

Para el diseño de trayectorias complejas y caóticas se han implementado sistemas que presenten atractores con múltiples enroscados. Este término, se utiliza para referirse a tres o más enroscados en un atractor visualizado en su espacio de fase. Un enfoque frecuente para generar uno o más enroscados, ha sido el de modificar un sistema que produce originalmente atractores con doble enroscado, como por ejemplo los sistemas de Chua y Lorenz, entre otros, añadiendo puntos de equilibrio al sistema para permitir que el flujo del sistema visite nuevas regiones en el espacio. Los atractores extraños de múltiple enroscado

aparecen como resultado de la combinación de varias trayectorias inestables “de una sola espiral" [6].

B. Sistemas lineales por pedazos.

Se consideró el siguiente sistema de ecuaciones dado por:

$$\dot{\boldsymbol{X}} = \mathbf{AX} + \mathbf{B}; \tag{1}$$

En donde $\boldsymbol{X} = [x, y, z]^T$ representa el vector del estado del sistema, $\boldsymbol{B} = [B_1, B_2, B_3]^T \in \mathbb{R}^3$ representa un vector real afín. $\boldsymbol{A} = [a_{i,j}] \in \mathbb{R}^{3x3}, i, j = 1, 2, 3$, denota una matriz real de coeficientes, la cual está dada por:

$$\boldsymbol{A} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1.5 & -1 & -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ B_3 \end{pmatrix}. \tag{2}$$

Para este caso en particular consideramos $B_1 = B_2 = 0$, ya que el punto de equilibrio así se desplazará únicamente en el eje x. Estamos interesados en un sistema disipativo que tenga un punto de equilibrio hiperbólico en $\boldsymbol{X}^*$, y debido a la simplicidad del sistema, estos se pueden calcular mediante $\boldsymbol{X}^* = -\mathbf{A}^{-1}\mathbf{B}$. En dónde el vector $\boldsymbol{B}$ conmutará dependiendo de la posición de $\boldsymbol{X}$, de tal forma que para cada valor conmutado en B_3 se generará un nuevo punto de equilibrio, tomando la siguiente forma:

$$B_3(\boldsymbol{X}) = \begin{cases} \beta_1, si\ \boldsymbol{X} \in D_1; \\ \beta_2, si\ \boldsymbol{X} \in D_2; \\ \quad . \\ \quad . \\ \beta_k, si\ \boldsymbol{X} \in D_k, \end{cases} \tag{3}$$

Donde $\beta_i \in \mathbb{R}$ y D_i corresponde a los dominios en donde se ubicarán cada enroscado del sistema. Cada enroscado estará asignado a su punto de equilibrio correspondiente $\boldsymbol{X}_1^* \in D_1, \ldots, \boldsymbol{X}_k^* \in D_k$ con $\boldsymbol{AX}_i^* + \boldsymbol{B}(\boldsymbol{X}) = 0, i = 1, \ldots, k$. El objetivo es elegir valores de β_i, de tal manera que el sistema sea estable y presente enroscados caóticos. En la Fig. 1, se muestra un diagrama de cómo están distribuidos los puntos de equilibrio marcados con puntos negros, los enroscados que se desea obtener mediante línea negra en espiral y las superficies de conmutación tanto del eje x como el de y marcadas como $\alpha_{-3}, \alpha_{-2}, \ldots, \alpha_3$ según la región.

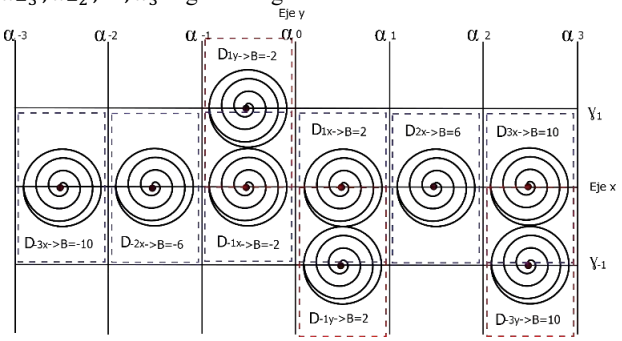


Fig. 1. Diagrama de regiones, superficies de conmutación y colocación de puntos de equilibrio para la realización del sistema multienroscado.

La ubicación de estas superficies de conmutación se da a conocer en la Tabla I:

TABLA I. Ubicación de las superficies de conmutación.

$\alpha_0 = 0$	
$\alpha_{-3} = -24/3$	$\alpha_3 = 24/3$
$\alpha_{-2} = -16/3$	$\alpha_2 = 16/3$
$\alpha_{-1} = -8/3$	$\alpha_1 = 8/3$
$\gamma_{-1} = -4/3$	$\gamma_1 = 4/3$

Estos valores se escogieron siguiendo la misma estructura de selección de los puntos de equilibrio que se presentan en [7]. Es importante mencionar que la distribución de estas superficies es simétrica, permitiendo que los enroscados generados presenten las mismas dimensiones. Cada espacio generado entre las superficies de conmutación corresponde con los dominios mencionados en la ec. (3). Para este caso se les asigna el nombre de $D_{-3x}, D_{-2x}, D_{-1x}, D_{1x}, D_{2x}, D_{3x}$ a los dominios que contienen un punto de equilibrio sobre el eje x, marcados con las casillas de línea punteada en azul en la Fig. 1. Para el caso de D_{-3y}, D_{-1y}, D_{1y}, marcados en recuadro con línea punteada roja, son los dominios que contienen un punto de equilibrio desplazado tanto en el eje x como en el y.

Dadas estas superficies de conmutación y los dominios en donde se desea la ubicación de los puntos de equilibrio, se diseña la siguiente ley de conmutación para el sistema de la ec. (1) con (2):

$$B_3 = \begin{cases} \beta_1\ si\ \{\alpha_0 \le \boldsymbol{X} < \alpha_1\ y\ \gamma_{-1} \le \boldsymbol{X} < \gamma_1\} \in D_{1x}; \\ \beta_2\ si\ \{\alpha_1 \le \boldsymbol{X} < \alpha_2\ y\ \gamma_{-1} \le \boldsymbol{X} < \gamma_1\} \in D_{2x}; \\ \beta_3\ si\ \{\alpha_2 \le \boldsymbol{X} < \alpha_3\ y\ \gamma_{-1} \le \boldsymbol{X} < \gamma_1\} \in D_{3x}; \\ \beta_4\ si\ \{\alpha_0 \ge \boldsymbol{X} > \alpha_{-1}\ y\ \gamma_{-1} \le \boldsymbol{X} < \gamma_1\} \in D_{-1x}; \\ \beta_5\ si\ \{\alpha_{-1} \ge \boldsymbol{X} > \alpha_{-2}\ y\ \gamma_{-1} \le \boldsymbol{X} < \gamma_1\} \in D_{-2x}; \\ \beta_6\ si\ \{\alpha_{-2} \ge \boldsymbol{X} > \alpha_{-3}\ y\ \gamma_{-1} \le \boldsymbol{X} < \gamma_1\} \in D_{-3x}; \\ \beta_7\ si\ \{\alpha_0 \ge \boldsymbol{X} > \alpha_{-1}\ y\ \gamma_1 \le \boldsymbol{Y} < \gamma_{-1}\} \in D_{-1y}; \\ \beta_8\ si\ \{\alpha_0 \le \boldsymbol{X} < \alpha_1\ y\ \gamma_1 \ge \boldsymbol{Y} < \gamma_{-1}\} \in D_{1y}; \\ \beta_9\ si\ \{\alpha_2 \le \boldsymbol{X} < \alpha_3\ y\ \gamma_1 \ge \boldsymbol{Y} < \gamma_{-1}\} \in D_{-3y}. \end{cases} \tag{4}$$

TABLA II. Posición de los puntos de equilibrio para la generación del sistema multienroscado.

Beta	$\boldsymbol{x}$	$\boldsymbol{y}$	$\boldsymbol{z}$
β_1	1.333	0	0
β_2	4	0	0
β_3	6.667	0	0
β_4	-1.333	0	0
β_5	-4	0	0
β_6	-6.667	0	0
β_7	-1.444	2.667	0
β_8	1.444	-2.667	0
β_9	6.778	-2.667	0

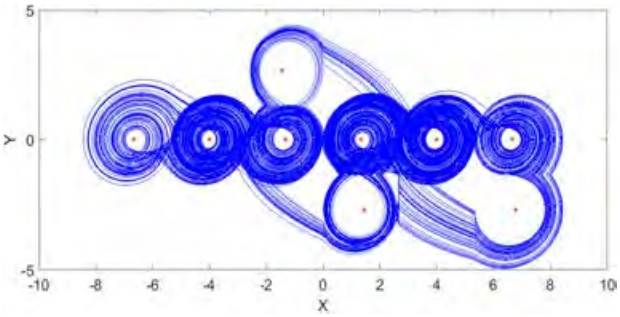


Fig. 2. Proyección del atractor dado por las ecs. (2) y (3) en el plano (x, y) para la ley de conmutación de la ec. (4) con nueve atractores.

Mediante esta ley de conmutación se puede obtener un atractor de 9 enroscados, tal y como se muestra en la Fig. 2. Note que la posición de dichos enroscados desplazados en el espacio, corresponde a lo propuesto en el diagrama de la Fig. 1. Los puntos de equilibrios obtenidos tras resolver $\boldsymbol{X}^* = -\mathbf{A}^{-1}\mathbf{B}$ con los valores de la ec. (4) se muestran en la Tabla II.
Ahora mediante este sistema propuesto se diseñará la llave para el proceso de encriptación como se muestra a continuación.

C. Generador de bits pseudoaleatorio.

Este generador se basa en las series de tiempo obtenidas a partir de los estados caóticos del sistema de multienroscados dados por las ecuaciones.

La idea es calcular la solución del sistema mediante algún método iterativo, como el método de Runge Kutta de 4to orden, y evolucionar el sistema n veces para obtener una secuencia $\boldsymbol{X}$ después de 1000 iteraciones del estado transitorio. Aprovechando la sensibilidad a las condiciones iniciales en sistemas caóticos, se considera que cada conjunto de ellas da como resultado diferentes series de tiempo. Por lo tanto, cada valor se puede considerar como una clave de cifrado, si se aumenta el número de enroscados, la dinámica del sistema es más compleja y la calidad del cifrado aumenta. A continuación, el generador de bits pseudoaleatorio (PRNG) se define similar a lo reportado en [1], de la siguiente manera:

$$Ki = \left| \sum_{j=1}^{4} X_j(i) \cdot 10^{14} \right| mod\ 256 \tag{3}$$

Aquí $\kappa_i \in \{0, 1, 2, \ldots, 255\}$ e $i = 1, \ldots, n$, donde $n = l \times m$ con l, m de acuerdo con el tamaño de la imagen en escala de grises a ser encriptado.

D. Diseño del esquema de cifrado y descifrado.

Después de crear las secuencias generadas por el sistema caótico con nueve atractores, encriptamos la imagen usando un cifrado de flujo similar a los descritos en [7,8]. El propósito de cifrar información con el PRBG propuesto es demostrar que las secuencias con diferente número de atractores generan una imagen de cifrado diferente, es decir, la calidad de encriptación mejora si se aumenta el número de atractores. El proceso para cifrar la imagen es píxel por píxel de la siguiente manera:

$$\begin{cases} C_1 = P_1 \oplus \kappa_1 \oplus IV \\ C_i = P_i \oplus \kappa_i \oplus C_{i-1} \end{cases} \tag{4}$$

Donde C_i y P_i con $i = 2, \ldots, n$ son los pixeles de la imagen de cifrado y la imagen normal, respectivamente. Para mejorar la seguridad en el proceso, se considera una retroalimentación en el cifrado (C_{i-1}) y un vector inicial, donde IV $\in \{0, 1, \ldots, 255\}$ es un vector de inicialización (Initial Vector) usado una vez para el primer pixel, κ_i es la secuencia de bits pseudoaleatoria, el símbolo $\oplus$ es la operación XOR, que se ejecuta bit a bit en el bloque de 8 bits por píxel.

Para descifrar correctamente la imagen, el receptor debe tener la misma corriente de claves (formada por las condiciones iniciales X_0, el vector de inicialización IV y la función de descifrado). Esta función toma la siguiente forma:

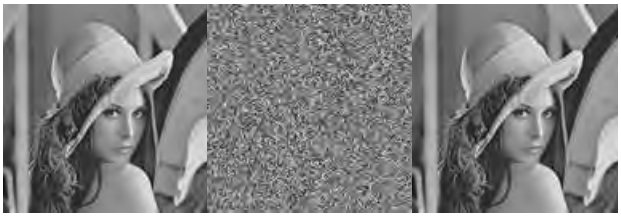
$$\begin{cases} P'_1 = C_1 \oplus \kappa_1 \oplus IV \\ P'_i = C_i \oplus \kappa_i \oplus C_{i-1} \end{cases} \tag{5}$$

Si se usan la clave correcta κ_i y el vector de inicialización correcto IV, entonces la imagen original se obtendrá correctamente, es decir, $P'_i = P_i$.

III. Resultados

A. Cifrado de la imagen.

Para probar el método de cifrado y descifrado, se consideró la imagen en escala de grises de Lena de 256x256 pixeles, por lo que la Fig. 3 (a) muestra la imagen original; la imagen de cifrado se presenta en la Fig. 3 (b) y la imagen descifrada se muestra en la Fig.3 (c).
Para estudiar la seguridad y calidad del proceso de encripción se implementaron los análisis del histograma y el estudio de la correlación entre imágenes que se describen a continuación.



a **b** **c**

Fig. 3. Imagen Lena: (a) original; (b) cifrada; (c) descifrada.

B. Análisis de histogramas.

El histograma muestra cómo se distribuyen los píxeles en una imagen. Traza el número de píxeles según el nivel de escala de grises. Una propiedad que debería satisfacer un sistema de encriptación es que el histograma de la imagen encriptada presenta una distribución uniforme. Por lo tanto, los histogramas entre la imagen original y la imagen encriptada deben ser completamente diferentes. La Fig. 4 muestra el histograma de la imagen original y la Fig. 5 muestra el histograma de la imagen cifrada. Es importante mencionar que este último representa una distribución uniforme como se esperaba.

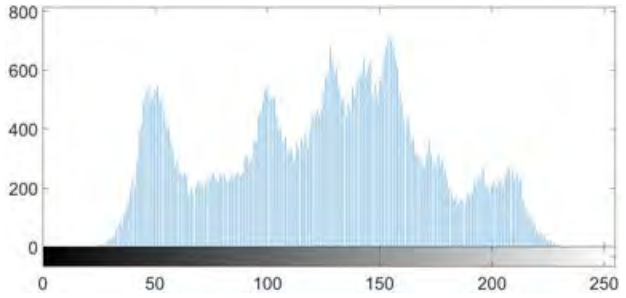


Fig. 4. Histograma de la imagen de Lena original.

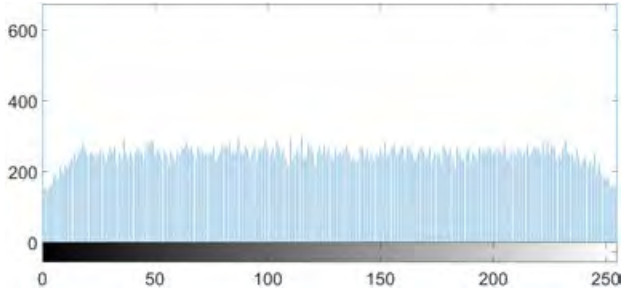


Fig. 5. Histograma de la imagen de Lena cifrada.

C. Análisis de correlación entre la imagen original y la encriptada.

Para mostrar que la imagen cifrada es independiente de la imagen simple, calculamos el coeficiente de correlación entre ambas imágenes. Si el coeficiente es cercano a 0, sugiere que no existe una correlación lineal o una correlación lineal débil. Los resultados para las imágenes en escala de grises se enumeran en Tabla II.

TABLA II. Coeficientes de correlación entre las imágenes simples y sus correspondientes imágenes cifradas.

Imagen	Coeficientes de correlación
Lena	0.0010040
Mandril	-0.0044883
Pimientos	-0.0036057

Podemos observar que los coeficientes son cercanos a cero (incluso para dos imágenes más Mandril y Pimientos que no se incluyeron en el trabajo por cuestión de espacio), mostrando que las imágenes simples son independiente de las respectivas versiones cifradas [9].

IV. CONCLUSIONES

En este trabajo presentamos un estudio de los sistemas lineales por pedazos produciendo atractores caóticos de multiple enroscado tanto en el eje x como el de y mediante la ubicación de los puntos de equilibrio. Las trayectorias caóticas que este atractor genera debido a su alta sensibilidad a las condiciones iniciales, fue utilizado para generar un vector de números aleatorios para el diseño de una llave para la encriptación de imágenes en escala de grises. Se sometió el sistema a pruebas para verificar la seguridad del cifrado y determinar si es confiable como medio de cifrado de información, saliendo favorecido por los análisis del histograma y la correlación entre la imagen original y la imagen cifrada. A futuro se planea someter el sistema a más pruebas de criptoanálisis y de esta manera determinar su seguridad y eficacia, así como implementar el estudio de incluir más puntos de equilibrio y de generar más enroscados al atractor. Así como estimar el tiempo de latencia y costo computacional de este sistema de cifrado.

V. AGRADECIMIENTOS

L.J. Ontañón García Pimentel agradece el apoyo recibido por el Proyecto FAI-UASLP con número de registro C18-FAI-05-45.45. A la SEP-PRODEP por el apoyo otorgado en UASLP-CA-268 con número de referencia IDCA 28234. Y al PFCE por el apoyo otorgado a la CARAO en el recurso P/PFCE 2018-24MSU0011E22.

VI. REFERENCIAS

[1] H. Cheng, Partial encryption of compressed images and videos, IEEE Trans. Signal Process. 48 (8) (2000) 2439–2451.

[2] N. Bourbakis, C. Alexopoulos, Picture data encryption using scan patterns, Pattern Recognit. 25 (6) (1992) 567–581.

[3] S. Wijaya, S.K. Tan, S.U. Guan, Permutation and sampling with maximum length CA or pseudorandom number generation, Appl. Math. Comput. 185 (1) (2007) 312–321.

[4] A.M.D. Rey, J.P. Mateus, G.R. Sánchez, A secret sharing scheme based on cellular automata, Appl. Math. Comput. 170 (2) (2005) 1356–1364.

[5] M. García-Martinez, L. J. Ontañón-García, E. Campos-Cantón, S. Čelikovský, Hyperchaotic encryption based on multi-scroll piecewise linear systems, Applied Mathematics and Computation 270 (2015) 413-424.

[6] Salgado Castorena, M. and Campos Cantón, E. (2016). Atractores caóticos con múltiple enroscado. Acapulco, Guerrero. 4° Encuentro de Jóvenes Investigadores – CONACYT. 11° Coloquio de Jóvenes Talentos en la Investigación.

[7] Ontanon Garcia, L. J., Jiménez López, E., Campos Cantón, E., y Basin, M. (2014). A family of hyperchaotic multi-scroll attractors in Rn. Applied Mathematics and Computation, 233, 522-533.

[8] H. Liu, X. Wang, A. Kadir, Color image encryption using choquet fuzzy integral and hyper chaotic system, Optik 124 (18) (2013) 3527–3533.

[9] X. Wang, J. Zhao, Z. Zhang, Chaotic encryption algorithm based on alternant of stream cipher and block cipher, Nonlinear Dyn. 63 (4) (2011) 587–597.

[10] M. T. Ramírez-Torres, J. S. Murguía, M. Mejía Carlos, Image encryption with an improved cryptosystem based on a matrix approach, International Journal of Modern Physics C Vol. 25, No. 10 (2014) 1450054.

ID óptico mediante QR-cifrados, patrones de difracción y marcas de agua

1st Alejandro Padrón-Godínez
Inst. y Medición, ICAT - Coord. Óptica
UNAM - INAOE
CDMX - Tonantzintla, Puebla - México
apadron@inaoep.mx

2nd Rafael Prieto Meléndez
Instrumentación y Medición, ICAT
UNAM
CDMX, México
rafael.prieto@ccadet.unam.mx

3rd Carlos Gerardo Treviño-Palacios
Coord. Óptica
INAOE
Tonantzintla, Puebla - México
carlost@inaoep.mx

***Resumen*—Las nuevas tecnologías han traído una diversidad de sistemas de seguridad implementadas tanto en software como en hardware portátiles para su uso como identificadores personales, algunos pocos ejemplos son tarjetas grabadas o con chips integrados, biométricos como lectores de huellas o iris. En este trabajo presentamos una mezcla entre implantación de mecanismos de seguridad y fenómenos físicos de propagación para el diseño de un dispositivo ID óptico que contenga información confidencial dentro de un código QR. La información dentro del código QR de pronta lectura esta cifrada mediante el algoritmo "Triple Data Encryption Standart"(FIPS46-3) de 8 bytes. La matriz de puntos del código QR genera una rejilla de difracción que produce patrones de difracción y sus correspondientes patrones entrelazados. Los patrones de difracción son insertados como marcas de agua mediante el proceso de daño óptico.**

***Palabras Clave*—criptografía, códigos-QR, difracción, marcas de agua**

I. Introducción

El diseño y construcción de sistemas seguridad de reconocimiento para control de acceso en la actualidad ya son más comunes y de uso diario, éstos son implementaciones en medios portátiles como identificadores personales, chips dentro de tarjetas de crédito, telefonía celular, computadoras, productos o activos para almacenamiento como las RFid, por mencionar algunos. Sin embargo, algunos dispositivos no tienen integrados los servicios y mecanismos de seguridad que permiten ingresar a un sistema o a lugares altamente confidenciales en forma segura. Lo recomendable es usar llaves públicas y privadas con generadores de secuencias pseudoaleatorias para que por medio de criptografía asimétrica ingresen de forma segura [1]. La mayor parte de los servicios de seguridad se logran mediante la implantación de algoritmos de cifrado, ya sea en hardware o software [2]. Algunos mecanismos como las marcas de agua son empleadas como candados en documentos valiosos, un ejemplo son los billetes de dinero para verificar su integridad y su autenticidad. Aunque la seguridad por obscuridad no es la forma de obtener dispositivos o medios seguros. La combinación de mecanismos de seguridad mediante Criptografía y Esteganografía trae consigo un aumento en el nivel de seguridad en el diseño de nuevos dispositivos portátiles de control de acceso [3]. La ventaja de la creación de los códigos QR de pronta lectura, es que fueran leídos por dispositivos portátiles electrónicos de almacenamiento para el manejo masivo de información como en el caso de levantamiento de un inventario [4]. Los QR fueron inventados por una empresa japonesa como sucesores de los códigos de barras, a nosotros nos interesan por dos razones, para guardar información confidencial cifrada en ellos y la generación de la matriz de puntos. La matriz de puntos a su vez genera una rejilla que al incidir sobre ella luz producirá el fenómeno de difracción, luego mediante el fenómeno de superposición de ondas electromagnéticas se tendrá su correspondiente patrón de difracción [5]. El patrón de difracción formado por la superposición tiene información de los códigos QR cifrados mediante el algoritmo 3DES [6]. En óptica física sabemos que el fenómeno de propagación sobre una apertura (rejilla de difraccón) es semejante a obtener la transformada de Fourier para obtener los patrones de difracción podemos producir imágenes en dos dimensiones de los patrones que serán nuestras marcas de agua [6]. Estas marcas de agua se insertarán o quemarán para hacer los dispositivos ID ópticos únicos a su correspondiente código QR cifrado, mediante el daño óptico sobre un cristal [7]. El esquema del procedimiento empleado se muestra en la Fig.(1). Para verificar la información se debe realizar el procedimiento inverso, escanear las marcas de agua producidas por los códigos QR, descifrar con el algoritmo 3DES para visualizar el texto plano. Debemos tener presente que las marcas de agua pueden ser perceptibles o imperceptibles dependiendo cuanta información se quiera ocultar en el patrón de difracción o el medio portador. En otros trabajos sobre marcas de agua imperceptibles en imágenes y en

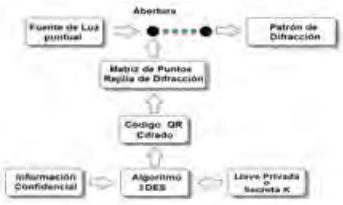


Fig. 1. Esquema para la generación del patrón de difracción generado por la abertura del código QR cifrado.

audio [8], [9], el procedimiento es procesar información para introducirla y ocultarla en un medio portador digital mediante algoritmos de inserción de forma imperceptible [10]. El patrón de difracción generado mediante la transformada de Fourier en dos dimensiones de la rejilla, es producido por la abertura y la propagación de radiación electromagnética a través de ella. Esto es lo que determina el procedimiento para ocultar la información y el fenómeno debe cumplir con las condiciones de interferencia mediante la superposición de ondas en un corte plano perpendicular a la dirección de propagación.

II. Servicios de Seguridad

Los servicios de seguridad (SS) que se manejan para el intercambio de información mediante un protocolo de comunicación son: confidencialidad, autenticidad, integridad, no repudio, control de acceso y disponibilidad [11]. No es posible implementarlos todos pero si se pueden implementar algunos gracias a los mecanismos de seguridad que han sido desarrollados hasta ahora. Estos pueden recordarse fácilmente en el triángulo de oro de la Fig. (2), (aunque en realidad se convierte en el tetraedro de oro). La Disponibilidad como SS está fuera del alcance de los mecanismos de seguridad, lo cual puede ser discutido en análisis subsecuentes de dichos mecanismos. El control de acceso dependerá del sistema de seguridad que se implemente [12].

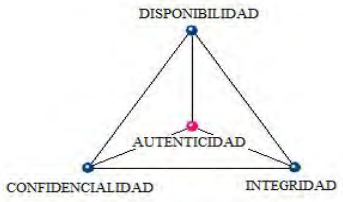


Fig. 2. Tetraedro de los servicios de seguridad.

III. Difracción

La radiación electromagnética representada en forma de luz se ha usado para explicar el fenómeno de interferencia en óptica, de acuerdo a que dos o más ondas coherentes individuales de luz, procedentes de una fuente única y separada por división de amplitud o frente de onda, se juntan para interferir. Particularmente, el mismo fenómeno está implicado en la difracción de la luz. La difracción es cualquier desviación de la óptica geométrica que resulta de la oclusión de un frente de onda de luz. Así una pantalla semitransparente con un orificio representa dicha oclusión y en una pantalla situada más allá del orificio, el círculo de la luz puede mostrar complejos efectos de borde. Este tipo de oclusión es común en muchos instrumentos ópticos que utilizan la parte de un frente de onda que pasa a través de una lente redonda. Una oclusión poligonal irregular muestra la estructura detallada en su propia sombra lo cual es inesperado sobre la base de la óptica geométrica. Efectos de difracción son una consecuencia del carácter de onda de la luz. Además si el obstáculo no es semitransparente, es decir, si éste causa transiciones locales en la fase o la amplitud del frente de onda de la luz transmitida, se observarán estos efectos. Ciertas imperfecciones en una lente producen patrones de difracción no esperados al transmitir luz láser. Debido a que se desvanecen los bordes de las imágenes ópticas por difracción, el fenómeno se limita a la precisión de la posición de los elementos del sistema como en el caso de los interferómetros. Si la fuente de luz tanto como la pantalla de observación están efectivamente lo suficientemente lejos de la abertura de difracción los frentes de ondas que llegan a la abertura y a la pantalla de observación pueden considerarse planos, se dice entonces que tenemos difracción de Fraunhofer o campo lejano; cuando éste no es el caso y la curvatura del frente de onda debe tomarse en cuenta para el cálculo del campo, tenemos difracción de Fresnel, o de campo cercano [13]. Para generar los patrones de difracción hacemos incidir luz láser sobre la matriz de puntos de los códigos QR cifrados en campo lejano [14]. Los patrones de difracción producidos son las marcas de agua generadas bajo el esquema que se mostró en la Fig.(1).

IV. Marcas de Agua

En el mundo digital, una MA es un patrón de bits insertados dentro de un medio digital que puede identificar al creador o a usuarios autorizados. La MA digital a diferencia del sello tradicional visible es diseñada para que sea invisible a la vista. Los bits insertados dentro de un audio digital o imagen son esparcidos por todo el documento (archivo) para evitar su identificación o modificación. Por lo que, la MA digital debe ser robusta y debe prevalecer a detecciones, compresiones y otras operaciones que pueden ser aplicadas al documento [8]. Entre los aspectos generales de las MA están la imperceptibilidad, seguridad, capacidad y robustez que son entre muchos aspectos necesarios para el diseño de las MA, el medio con MA debe ser indistinguible del medio original sin alterar, Fig.(3). Un sistema MA ideal debe insertar

Fig. 3. Marcas de agua sobre a) billetes, b) imagénes y c) videos.

una gran cantidad de información perfectamente segura, pero sin degradación visible en el medio huésped. La MA debe ser robusta ante ataques de variaciones intencionales (recorte, redimensionamiento o compresión) y no intencionales (ruido) [9]. Muchas investigaciones se han enfocado sobre seguridad y robustez, pero raramente sobre la capacidad de las MA. La cantidad de datos que un algoritmo puede introducir en un medio tiene implicaciones para como las MA pueden ser aplicadas. En efecto, ambas seguridad y robustez son importantes debido a que la MA insertada se espera que sea imperceptible e irremovible, si una MA grande puede ser introducida dentro de un medio huésped, el proceso debería ser empleado para muchas otras aplicaciones [10].

V. METODOLOGÍA

El primer paso es cifrar la información confidencial o texto plano, pueden ser datos personales, con el algoritmo 3DES. Un segundo paso es generar el código QR correspondiente con esta información cifrada. En el tercer paso la matriz de puntos creada en el código QR es una imagen digital en blanco y negro en mapa de bits de 256 colores de 400x400 pixeles, hay que convertirla en una imagen de mapa de bits monocromática para que podamos usarla como rejilla de difracción. Para generar una rejilla de difracción o abertura usaremos dos técnicas, una es a través del modelo matemático de la abertura, la otra es a través directamente de la imagen del código QR cifrado y simular la propagación sobre ellas. Realizaremos varios casos, en el primero generamos la abertura de la letra "A" con los tres cuadros de referencia del código QR. Entonces con la siguiente expresión:

$$\begin{aligned} Ap_x &= rect((X)/(4*\delta)) * rect((Y-10)/(\delta)) + \\ &\quad rect((X)/(4*\delta)) * rect((Y+10)/(\delta)) \\ Ap_y &= rect((X-15)/\delta) * rect((Y+10)/(4*\delta)) + \\ &\quad rect((X+15)/(\delta)) * rect((Y+10)/(4*\delta)), \end{aligned} \quad (1)$$

y sumando estas expresiones $Ap = Ap_x + Ap_y$ se tiene la letra "A". Con la función rect(X, Y) en el intervalo de [-1/2,1/2] y con constantes $\delta = 10$; la forma de esta abertura se muestra en la Fig.(4), después se mostrará como código QR, Fig.(7). Una vez que tenemos los modelos matemáticos o

Fig. 4. Representación del modelo matemático de una abertura tipo "A".

bien las imágenes de las aberturas definidas, podemos propagar la radiación electromagnética a través de ellas emitiendo luz desde una fuente puntual y colocando abertura y pantalla de observación en difracción de Fraunhofer o campo lejano. Para esto usamos la función de onda en dos dimensiones mediante la siguiente ecuación para la propagación del campo y encontrar la irradiancia emitida:

$$\Psi(f_x, f_y, z) = \frac{e^{ikz}}{i\lambda z} \iint_A \Psi_A(x,y)\, e^{-i\,2\pi(f_x x + f_y y)}\, dx.dy \quad (2)$$

donde $\psi_A(x,y)$ es la abertura y f_x y f_y están relacionadas con las frecuencias espaciales, λ la longitud de onda, k el vector de onda, z la dirección de la propagación. La ecuación (2) se puede obtener a partir de la integral de superficie de Fresnel-Kirchhoff usada para la difracción sobre aberturas con simetría rectangular [13], Fig.(5). Cuando la integral se define sobre el intervalo $[-\infty, \infty]$ se convierte en la transformada de Fourier de la abertura, $\mathcal{F}(\psi_A(x,y))$. El resultado de la solución de la integral de propagación es el patrón de difracción generado sobre la pantalla de observación y para el patrón entrelazado se calcula el logaritmo en base 2 de la Transformada de Fourier resultante.

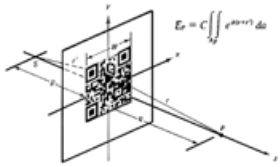


Fig. 5. Sistema de difracción de las aberturas para las Marcas de Agua.

VI. RESULTADOS

Al inicio de esta sección mostramos los códigos QR con cifrado y sin cifrado para observar la diferencia entre sus matrices de puntos, Fig.(6). Usaremos la clave privada "Santiago" 8-Bytes o 64-bits, que forman una palabra de 8 caracteres para el algoritmo de cifrado 3DES. Luego utilizaremos cuatro

Fig. 6. Cdigos QR con a) texto plano y b) texto cifrado para las aberturas.

matrices de puntos con información cifrada como rejillas de difracción que juegan el rol de abertura para obtener los patrones de difracción y sus correspondientes patrones entrelazados. Ahora se muestran figuras del código QR cifrado, patrón de difracción alias marca de agua y su patrón entrelazado de los cuatro casos de estudio en este trabajo, Fig.(7, 8, 9, y 10). Los patrones de difracción son tenues, que

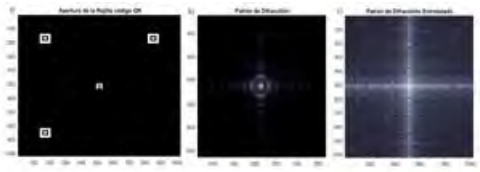


Fig. 7. a) Código QR con la letra A, b) patrón de radiación y c) patrón de radiación entrelazado.

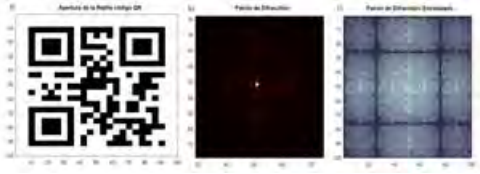


Fig. 8. a) Código QR cifrado del texto plano: 2018RCI4, b) patrón de radiación y c) su correspondiente patrón de radiación entrelazado.

es lo que muestra la inserción de una marca de agua poco perceptible, sin embargo en el patrón de difracción entrelazado es más perceptible. Aunque sólo es eso una mancha donde a

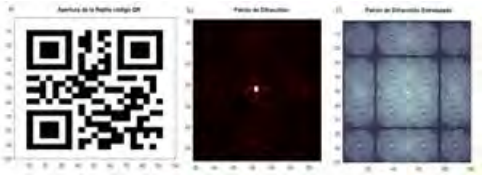


Fig. 9. a) Código QR cifrado del texto plano: ABCDEFGH, b) patrón de radiación y c) su correspondiente patrón de radiación entrelazado.

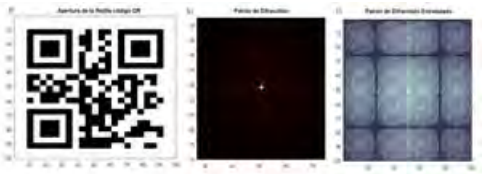


Fig. 10. a) Código QR cifrado del texto plano: INAOEPUE, b) patrón de radiación y c) su correspondiente patrón de radiación entrelazado.

simple vista no puede detectarse nada. La mayor parte de la información en los patrones de difracción se muestra en los centros de las imágenes, debido al método de la transformada discreta de Fourier que se utiliza para hacer la propagación de la luz incidente sobre las aberturas. Algo de lo que pudimos percatarnos con los lectores de códigos QR es que no importa si la matriz de puntos es el negativo o el positivo, ellos siempre leen la misma información. Lo que a continuación mostramos es como quedaría el dispositivo ID óptico usando la técnica de grabado mostrada en la referencia [15], para el grabado de las marcas de agua y que efectivamente se pueda grabar un holograma dentro de un cristal. Este holograma contiene la información que nosotros deseamos asegurar mediante el cifrado en los códigos QR y ocultados como MA en los patrones de difracción. La Fig. (11) es una muestra de la factibilidad del dispositivo.

Fig. 11. Hologramas creados y grabados dentro de un cristal (las dos imágenes de la izquierda). Un código QR con logotipo y su grabado (las dos imágenes de la derecha).

VII. Conclusiones

La intención de producir un dispositivo con información confidencial cifrada es para generar un dispositivo ID óptico como una clave privada de control de acceso portable casi como una huella digital sin depender de generadores de secuencias dinámicas pseudoaleatorias. El dispositivo de lectura o reconocimiento tiene que realizar el proceso inverso para captar el texto en claro procedente de la información oculta y cifrada, y conocer la clave secreta que se uso en el algoritmo 3DES. La seguridad que presentamos es: cualquiera puede leer la información formada en la matriz de puntos del código QR, pero no cualquiera la puede descifrar sin la clave privada aún sabiendo que hay información oculta en el patrón de difracción entrelazado o estego-objetos cifrados que mostramos en los resultados. El dispositivo creado como un medio portador de la información clasificada cifrada, contiene mecanismos de seguridad (algoritmo criptográfico 3DES), y hablando de los SS pueden emplearse como control de acceso, autenticidad, no repudio e integridad, [6]. Las características y pruebas de los grabados las dejamos para un trabajo futuro, ya que dependemos de una buena calibración y alineación de la óptica involucrada y de la potencia del láser que emplearemos para el daño óptico. Así como las dimensiones, longitudes de onda y del material para el medio portador.

Agradecimientos

Este trabajo ha sido financiado por la Dirección General de Personal Académico de la Universidad Nacional Autónoma de México bajo el Programa de Apoyos para la Superación del Personal Académico a través de la beca doctoral.

Referencias

[1] QR codes. Available at: “https://es.wikipedia.org/wiki/Código-QR,” Aug,23,2017.
[2] Daltabuit E., Hernández L., Mallén G., Vázquez J., “La seguridad de la Informacin,” Ed. Limusa, 2007.
[3] Meneses A. J., Van Oorschot P. C., Vanstone S. A., “Hanbok of Applied Cryptography”, CRC, 2000.
[4] FIPS Publication 46-3, (1999). Data Encryption Standard (DES).
[5] INTERNATIONAL STANDARD, ISO/IEC 18004, “Information technology - Automatic identification and data capture techniques - Bar code symbology QR Code,” First edition 2000-06-15.
[6] INTERNATIONAL STANDARD, ISO 7498-2, “Information processing - Open Systems Interconnection - Basic Reference Model. Security Architecture,” First edition 1989-02-15.
[7] Padrón Godínez A., Azuara Pérez L., Prieto Meléndez R., Herrera Becerra A. A., “Robustez de Marcas de Agua ante ataques,” XXIV Congreso de Instrumentación, Mérida, Yucatán, México, 2009, 6 páginas.
[8] Padrón Godínez A., González Lee M., Prieto Meléndez R., Herrera Becerra A. A., “Marcas de Agua Imperceptibles en Audio Digital,” SOMI XXIII Congreso de Instrumentación, Sociedad Mexicana de Instrumentación, Xalapa, México, octubre de 2008, 7 páginas.
[9] Padrón Godínez A., González Lee M., Prieto Meléndez R., Herrera Becerra A. A., “Ocultamiento de Datos en Imagénes Digitales Mediante BPCS”. SOMI XXIII Congreso de Instrumentación, Sociedad Mexicana de Instrumentación, Xalapa, México, octubre de 2008, 6 páginas.
[10] Shih F. Y., “Digital Watermarking and Steganography,” CRC Press, USA, 2008.
[11] In-Kwon Yeo, Hyoung Joong Kim. “Modified Patchwork Algorithm: a novel audio watermarking scheme,” Information Technology Coding and Computing, 2001. Proceedings. International Conference on Volume, Issue, Apr 2001 Page(s):237242, Digital Object Identifier 10.1109/ITCC.2001.918798.
[12] Houtsma, A. J. M., Rossing T. D., “Auditory Demonstrations,” Institute of Perception Research, 1987. Folleto del CD “Auditory Demonstrations,” Philips 1126-061.
[13] Pedrotti F. L. and Pedrotti L. S. “Introduction to Optics”, Ed. Prentice-Hall Int. Inc., USA, 1993.
[14] Treviño-Palacios C. G., Olivares-Pérez A., Zapata-Nava O.J., “Optical damage as a computer generated hologram recording mechanism,” Journal of Applied Research and Technology 13 (2015) 591595
[15] Treviño-Palacios C. G., Olivares-Pérez A., Zapata-Nava O.J., “Security system with optical key Access,” Proc. of SPIE Vol. 6422 642218-1, 2007.

Criptoanálisis y mejora a sistema de cifrado hipercaótico para imágenes

M. T. Ramírez-Torres
Coordinación Académica Región Altiplano Oeste
Universidad Autónoma de San Luis Potosí
San Luis Potosí, México
tulio.torres@uaslp.mx

C. A. Guerra García
Coordinación Académica Región Altiplano Oeste
Universidad Autónoma de San Luis Potosí
San Luis Potosí, México
cesar.guerra@uaslp.mx

C. Montalvo
Facultad de ingeniería
Universidad Autónoma de San Luis Potosí
San Luis Potosí, México
carlos.soubervielle@uaslp.mx

***Abstract*— En los últimos años, ha habido iniciativas para aplicar diferentes sistemas caóticos a la criptografía. En la propuesta mostrada por García-Martínez et al, los autores mostraron un nuevo sistema de cifrado basado en un PRBG (Pseudo Random Bit Generator), capaz de generar secuencias binarias utilizando los cuatro estados de un sistema hipercaótico multienroscado. Aun cuando esta propuesta se evaluó a través de seis pruebas de seguridad (análisis de espacio clave, entropía…etc.) este sistema presenta una debilidad, al momento de aplicar un ataque de imágenes en claro elegidas, conocido como Chosen Plain Image Attack (CPIA). En este trabajo se presenta un criptoanálisis al sistema y una propuesta de mejora.**

Keywords—Criptoanálisis, vulnerabilidad, ataque.

I. Introducción

En la actualidad, debido a la demanda de seguridad de la industria 4.0, por todos los procesos que requieren trabajar en línea, y el almacenamiento seguro de información confidencial, se han propuesto diversos algoritmos criptográficos con diferentes enfoques, destacando los de caótico. Esto debido a propiedades que tienen como, ergodicidad y la sensibilidad a condiciones iniciales. Sin embargo en muchas ocasiones estos nuevos sistemas presentan debilidades ante ataques de criptoanálisis y/o criptoanálisis diferencial. Provocando la fuga de información confidencial. Por ejemplo en [1], utilizan una secuencia pseudoaleatoria generada por un sistema hipercaótico para cifrar las imágenes, utilizando la operación XOR y la suma modular. Este sistema fue analizado en [2] y se encontraron debilidades al momento de aplicar el ataque CPIA. Por otra parte, en [3] se propuso un método de cifrado y de generación de cajas de sustitución basado en caos. Sin embargo en 2018, se publicó en [4], las debilidades del sistema propuesto por Çavuşoğlu et. al, bajo el ataque chosen-plaintext attack. En [5] los autores proponen un algoritmo de cifrado de imágenes caótico, basado en la entropía de la información. En el mismo año, Li et. al, en [6] revelan los problemas de seguridad que presenta dicho sistema ante ataques diferenciales. Por lo que podemos ver que es necesario un análisis mas profundo en diferentes escenarios, para poder validar un nuevo sistema de cifrado.

Para el cifrado de imágenes existen diversas consideraciones, debido a propiedades intrínsecas de éstas, como una gran tasa de datos y una alta correlación adyacente. Por lo tanto los algoritmos propuestos para estas áreas deben cumplir con dos tipos de seguridad: criptográfica y perceptual[7]. Algunos nuevos sistemas se enfocan solo en la seguridad perceptual y los autores validan sus resultados con pruebas estadísticas. Descuidando aspectos de seguridad ante otro tipo de ataques.

Por lo tanto, en este trabajo se busca ilustrar de manera explicita, una forma de llevar a cabo el ataque CPIA y una forma de mejorar el sistema de cifrado analizado. Buscando que futuros desarrolladores consideren estas pruebas y diseñen algoritmos de cifrado resistentes y eficientes. Este artículo se conforma de la siguiente manera, en la sección II se describe el sistema de cifrado propuesto por García-Martínez, mientras que en la sección III se detalla el proceso de criptoanálisis. En la sección IV se muestra la mejora que se propone y un breve análisis. Y en la sección V se encuentran las conclusiones.

II. Sistema de cifrado

García-Martínez propuso un sistema de cifrado para imágenes en escala de grises en el trabajo [8]. Hace uso de un nuevo PRBG que produce secuencias binarias, utilizando cuatro estados de un sistema hipercaótico multienroscado.

Las imágenes son cifradas pixel a pixel utilizando las siguientes ecuaciones:

$$\begin{cases} C_1 = P_1 \oplus k_1 \oplus \boldsymbol{IV} \\ C_i = P_i \oplus k_i \oplus C_{i-1} \end{cases}, \quad (1)$$

donde C y P represntan los pixeles cifrados y en claro respectivamente, con $i = 2..n$. $\boldsymbol{IV}$ representa un vector inicial de 8 bits, k es una secuencia aleatoria de 8 bits obtenida del PRBG. Y por último, el símbolo $\oplus$ representa la operación XOR. Para obtener el primer pixel cifrado C_1, se calcula una operación XOR entre el coeficiente del pixel P_1, la secuencia aleatoria k_1 y el vector inicial $\boldsymbol{IV}$. Los siguientes pixeles cifrados C_i, se obtiene realizando una operación XOR entre el coeficiente del pixel P_i, una nueva secuencia aleatoria k_i y el pixel cifrado previo C_{i-1}. Este proceso se repite hasta cifrar

todos los pixeles de la imagen. Las condiciones iniciales del PRBG funcionan como llave secreta.

Como podemos observar el esquema cifra directamente los coeficientes de los pixeles, sin utilizar una operación de sustitución previamente, esto permite a los atacantes introducir datos de manera arbitraria.

III. Criptoanálisis

En el ataque Chosen Plain Image Attack, el atacante es capaz de seleccionar las imágenes en claro y obtener sus respectivas versiones cifradas, sin embargo no posee la llave secreta. Este ataque fue aplicado al esquema de García-Martínez, como se describe en [9]. Para ilustrar este proceso, vease la Fig. 1. El ataque comienza seleccionando las dos imágenes en claro, en este caso se utiliza la imagen de Lena, Fig. 1a), y una imagen solida negra, Fig. 1b). Ciframos ambas imágenes con el algoritmo de García-Martínez con las mismas condiciones iniciales, y las imágenes que se obtienen son, Fig. 1c), Lena cifrada, y la Fig. 1d), la imagen solida cifrada, la cual llamaremos Mascara $\boldsymbol{I}_M$. Para recuperar la imagen de Lena sin conocer las condiciones inciales basta con calcular una operación XOR entre ambas imágenes cifradas, pixel a pixel. El resultado lo podemos ver en la Fig. 1e), que como se puede ver esta imagen revela patrones muy significativos de la Fig. 1a). Aun así el proceso de recuperación se puede mejorar, nuevamente sin conocer las condiciones iniciales y la imagen se puede recuperar al 100%, como se puede ver en la Fig. 1f). El proceso para obtener esta imagen será explicado más adelante.

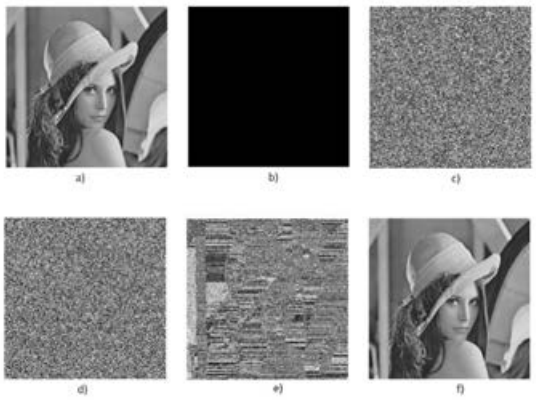


Fig. 1. Chosen Plain Image Attack. a) Imagen de Lena, b)imagen solida negra, c)imagen de Lena encriptada, d)máscara, e) imagen recuperada con la operación XOR, f) imagen recuperada usando (3).

Este ataque funciona en este esquema, posiblemente por varias razones, pero este trabajo se enfoca en la falta de una función de sustitución, para evitar que el adversario introduzca valores en las ecuaciones a su conveniencia. Para ilustrar la debilidad observemos (2), esta ecuación representa el paso del ataque, donde se hace la operación XOR pixel a pixel.

$$C_{L1} \oplus C_{M1} = (P_{L1} \oplus k_1 \oplus \boldsymbol{IV}) \oplus (0 \oplus k_1 \oplus \boldsymbol{IV}) = P_{L1} \quad (2)$$

Donde C_{L1} representa el primer pixel de la imagen de Lena cifrada, C_{M1} representa el primer pixel de la Mascara $\boldsymbol{I}_M$. Y por último, P_{L1} representa el primer pixel de la imagen de Lena. Como se puede ver, al momento de calcular la operación XOR entre ambos pixeles, los elementos de la ecuación de cifrado se reducen aplicando algebra booleana, y el resultado es el coeficiente P_{L1}. Para recuperar los demás pixeles se utiliza (3), esta versión es la usada en la Fig. 1f). Para mejorar su desempeño en la recuperación, agregamos una operación XOR entre los pixeles cifrados previos, adicional a la de pixel a pixel, como se muestra a continuación:

$$(C_{Li} \oplus C_{Mi}) \oplus (C_{Li-1} \oplus C_{Mi-1}) = P_{Li}, \quad (3)$$

como se puede ver, es posible recuperar la imagen original, sin conocer la llave secreta.

IV. Mejora propuesta

Para mejorar el sistema se propone agregar una función de preprocesamiento, capaz de sustituir el texto plano antes de ser cifrado. Sin importar que el texto en claro sea altamente redundante, esta función debe intercambiarlo por diferentes valores de la codificación, con igual probabilidad. Si se desea utilizar una caja de sustitución, el algoritmo debería modificarse, ya que simplemente intercambiar el texto con una S-box antes de cifrar, crearía patrones de la imagen original.

La función de preprocesamiento utilizada en esta mejora fue diseñada en [10]. Esta función se basa en la sincronización de autómatas celulares, usando la regla local 90. Es una modificación de un generador de números pseudoaleatorios propuesto en [11]. Gracias a su retroalimentación, la función de preprocesamiento puede intercambiar valores idénticos por números diferentes en cada iteración.

Para explicar su funcionamiento, en la Fig. 2 se ilustra el generador pseudoaleatorio y el proceso de evolución hacia atrás usando la regla 90. Se utiliza un vector $\boldsymbol{x}$ y un vector $\boldsymbol{y}$ de n bits y $n+1$ bits, respectivamente. Se evoluciona hacia atrás, utilizando la operación XOR como indican las flechas, hasta generar el vector $\boldsymbol{t}$. Esta función es llamada h.

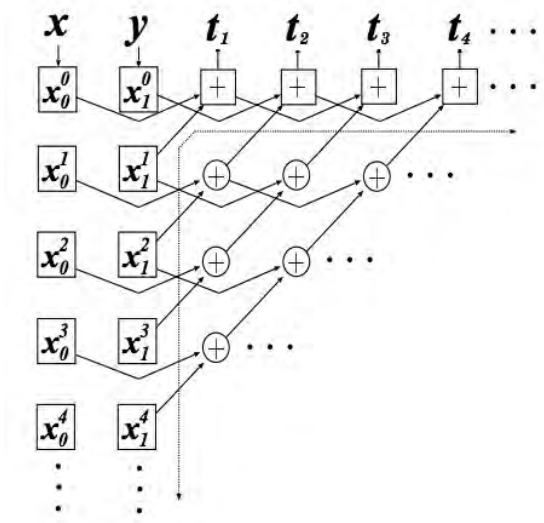


Fig. 2. Generador de secuencias pseudoaleatorias $\boldsymbol{t}$ de n bits, basado en la evolución hacia atrás de la regla 90.

Identify applicable funding agency here. If none, delete this text box.

Para aplicar esta operación como función de preprocesamiento, en la Fig. 3, podemos observar a la función h como un bloque, y en el lugar del vector $\boldsymbol{x}$, entra el coeficiente del pixel $\boldsymbol{p}$, y en el lugar del vector $\boldsymbol{y}$, un nuevo vector llamado $\boldsymbol{z}$. Esto para diferenciar su funcionamiento como generador de números pseudoaletorios y como función de preprocesamiento. El vector de salida es llamado $\hat{\boldsymbol{p}}$, para señalar que es la versión procesada de $\boldsymbol{p}$.

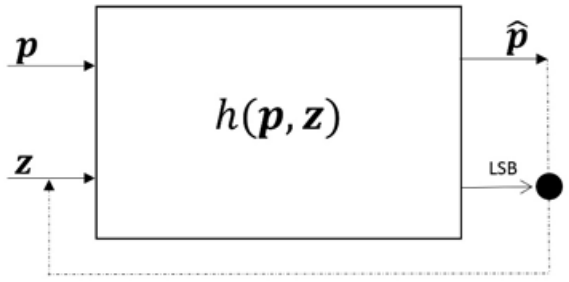


Fig. 3. Función de preprocesamiento. $\boldsymbol{p}$ es el coeficiente del pixel, $\boldsymbol{z}$ un vector aleatorio. A la salida se obtiene el vector preprocesado $\hat{\boldsymbol{p}}$.

Como se puede ver existe una retroalimentación que actualiza el vector $\boldsymbol{z}$, este nuevo vector se calcula con el vector de salida $\hat{\boldsymbol{p}}$, concatenando el bit menos significativo del vector $\boldsymbol{z}$, en la posición de bit más significativo.

La diferencia entre esta función y una caja de sustitución la podemos observar en la Fig. 4.

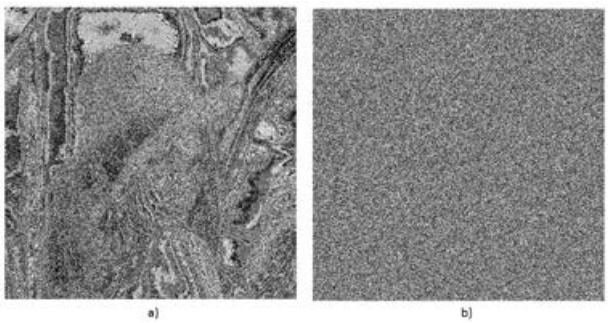


Fig. 4. a) imagen de Lena sustituida con una S-box del sistema AES (Advanced Encryption Standar), b) imagen de Lena despues de ser preprocesada con la función h.

Se puede observar que en el caso de la caja se sustitución se crean patrones, debido a que no existe ningún tipo de dinámica, los coeficientes de la imagen son sustituidos siempre por los mismos valores de la S-box.

En la Fig. 5 se muestra el histograma de la imagen de Lena y su versión preprocesada. Como se puede ver el histograma se vuelve uniforme, ocultando la redundancia de la imagen original y previniendo un ataque estadístico.

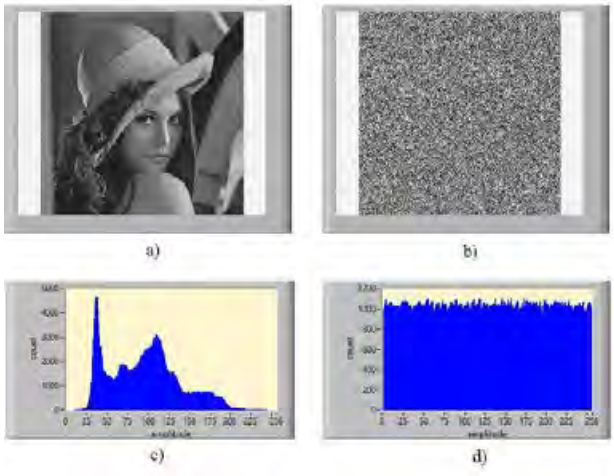


Fig. 5. Análisis de histogramas. a) Imagen de Lena, b)imagen preprocesada de Lena, c)histograma de a) y d)histograma de b).

Agregar la función de preprocesamiento al algoritmo de García-Martínez, antes del cifrado, mejora su desempeño ante el ataque CPIA. Lo anterior se puede confirmar en la Fig. 6, donde nuevamente se escogen las mismas dos imágenes de forma arbitraria.

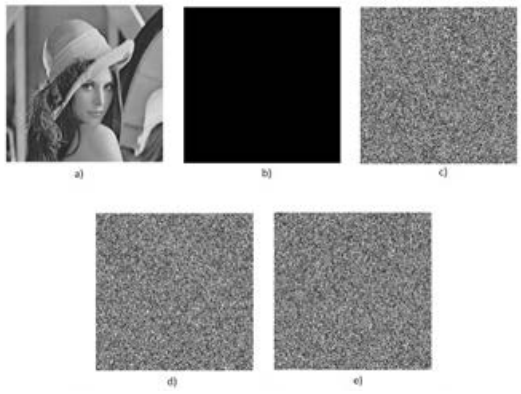


Fig. 6. Chosen Plain Image Attack. a) Imagen de Lena, b)imagen solida negra, c)imagen de Lena encriptada, d)máscara, e) imagen recuperada con la operación XOR.

Como podemos observar el atacante no puede introducir el valor de 0 de forma arbitraria en las ecuaciones de cifrado, esto evita que capture información en la Mascara $\boldsymbol{I_M}$. Además la información no está cifrada de manera directa, el preprocesamiento intercambia los valores, por lo tanto ante condiciones que se dan en este ataque, no queda expuesta la información.

V. Conclusiones

Los sistemas caóticos pueden aportar elementos en el diseño de sistemas de cifrado. Sin embargo, su análisis debe ser profundo e interpretar de manera general las pruebas que se aplican a los esquemas de cifrado. Ya que en algunos casos la

fundamentación para realizar de cierta manera una prueba es porque se copia de otro trabajo, sin analizar los supuestos que considera el ataque y que las condiciones cambian en cada sistema de cifrado.

El cifrado de imágenes sigue presentado áreas de oportunidad y desarrollo, porque cuando un sistema logra solventar las problemáticas de seguridad incrementa su latencia. Por lo que la búsqueda de nuevos métodos se mantiene aún en auge y los sistemas caóticos pueden brindar soluciones a este problema.

Referencias

[1] C. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences" *Optics communications*, 2012, vol. 285, pp. 29-37, Jan. 2012.

[2] C. Li, Y. Liu, T. Xie, M. Z Chen, "Breaking a novel image encryption scheme based on improved hyperchaotic sequences" *Nonlinear Dynamics*, vol. 73, pp. 2083-2089, May 2013.

[3] Ü. Çavuşoğlu, et al. "Secure image encryption algorithm design using a novel chaos based S-Box" *Chaos, Solitons & Fractals*, vol. 95, pp. 92-101, Feb. 2017.

[4] C. Zhu, G. Wang, K. Sun, "Cryptanalysis and improvement on an image encryption algorithm design using a novel chaos based S-box" *Symmetry*, vol. 10, pp. 399. Sept. 2018.

[5] G. Ye, C. Pan, X. Huang, Z. Zhao, and J. He, ''A chaotic image encryption algorithm based on information entropy'' *Int. J. Bifurcation Chaos*, vol. 28, 2018.

[6] C. Li, et al. "Cryptanalysis of a chaotic image encryption algorithm based on information entropy" *IEEE Access*, vol. 6, pp. 75834-75842, 2018.

[7] S. Lian, *Multimedia content encryption: techniques and applications*, Auerbach Publications, 2008.

[8] M. García-Martínez, L. J. Ontañón-García, E. Campos-Cantón, & S. Čelikovský, "Hyperchaotic encryption based on multi-scroll piecewise linear systems" *Applied Mathematics and Computation*, vol. 270, pp. 413-424, Nov. 2015.

[9] S. Li, C. Li, G. Chen, & K. T. Lo, "Cryptanalysis of the RCES/RSES image encryption scheme." *Journal of Systems and Software*, vol. 81, pp. 1130-1143, Jul. 2008.

[10] M. T. Ramírez-Torres, J. S. Murguia, M. Carlos Mejía, "Image encryption with an improved cryptosystem based on a matrix approach." *International Journal of Modern Physics C*, vol. 25, pp. 1450054, Apr. 2014.

[11] J. Urias, E. Ugalde, G. Salazar, "A cryptosystem based on cellular automata," *Chaos*, vol. 8, pp. 819-822, Dec. 1998.

Implementación de una plataforma de comunicación cifrada en FPGA

1st Alejandro Padrón-Godínez
Inst. y Medición, ICAT - Coord. Óptica
UNAM - INAOE
CDMX - Tonantzintla, Puebla - México
apadron@inaoep.mx

2nd Rafael Prieto Meléndez
Instrumentación y Medición, ICAT
UNAM
CDMX, México
rafael.prieto@ccadet.unam.mx

3rd Carlos Gerardo Treviño-Palacios
Coord. Óptica
INAOE
Tonantzintla, Puebla - México
carlost@inaoep.mx

***Resumen*—Para realizar una comunicación cifrada o bien una comunicación segura que no se pueda alterar, modificar, robar su contenido es necesario que en los protocolos de comunicación esten bien definidas las tareas que deben de ejecutar cada entidad participante. En este sentido detectamos dos sitemas entrelazados que nos ayudan a proporcionar servicios de seguridad, uno el sistema de comunicación y otro el protocolo de comunicación. En este trabajo presentamos una plataforma de comunicación cifrada implementada en sistemas de lógica programable. Esta plataforma contiene elementos de transmisión y recepción de información además de un mecanismo de cifrado/descifrado para realizar una comunicación segura. El mecanismo de cifrado/descifrado es el algoritmo criptográfico por flujo o bloques acondicionado como flujo que podemos intercambiar en la plataforma, los cuales son desarrollados en lenguaje de descripción de hardware. Realizamos la validación de la plataforma usando el algoritmos $A5\_1$ tipo Vernam.**

***Palabras Clave*—criptografía, sistemas de lógica programable FPGA, comunicación serial.**

I. Introducción

La diversidad de sistemas de seguridad implementados tanto en software como en hardware ahora son muy comunes, sin embargo las plataformas donde se instalan estas aplicaciones no son tan seguras. Podemos recordar aquello que: "seguridad por obscuridad no es seguridad" y muchos sistemas actuales pueden ser criptoanalizados conociendo las vulnerabilidades de las plataformas y también de quien las manejan [1]. Los sistemas de comunicación que usualmente son empleados para transmitir información viaja en forma clara desde su origen hasta su destino. Algunas veces se usan protocolos de comunicación seguros pero sobre una plataforma que no es segura. Como parte del desarrollo de nuestro laboratorio estamos interesados en transmitir comandos y señales bajo una plataforma segura tratando que la información cifrada alcance su destino sin alteraciones y pueda ser descifrada sin problema. En el proceso lo deseable es no afectar o modificar el sistema de comunicación empleado en tiempo real, en términos de velocidad y calidad de transmisión [2], Fig. (1). En la construcción de la plataforma, cualquier implementación de un mecanismo de seguridad en lenguaje de descripción de hardware, debe ser transparente al usuario pero debe de darse cuenta que la información esta cifrada bajo

PASPA-DGAPA-UNAM beca de doctorado.

Figura 1. Spartan 3E con dos puertos seriales.

el mecanismo en cuestión para poder aplicar su descifrado y obtener el mensaje en claro. La implementación del sistema de comunicación intercambia información mediante el protocolo de comunicación serial $RS-232$, la cual generalmente es en ambas direcciones (full-duplex), entre dos tarjetas Spartan 3E fabricadas por Xilinx. En la plataforma ya se han evaluado algunos algoritmos de cifrado como un AES con modos de operación contador y bloques de retroalimentación (CFB), [3], [4]. Así como generadores de números pseudoaleatorios a partir de registros de desplazamiento retroalimentados lineales (LFSR por sus siglas en ingles) [5]. En este trabajo probamos el algoritmo $A5_1$ para telefonía celular [6]. En particular la implementación del algoritmo se lleva a cabo en Lenguaje de Descripción de Hardware (VHDL) sobre los sistemas de lógica programable (FPGA).

II. Características de la plataforma

La seguridad de los sistemas de comunicación depende mucho de que tan vulnerable sea el medio de transmisión y como puede verse afectado ante ataques pasivos y activos. En consecuencia debemos enumerar las características que debe cumplir la plataforma para su buen funcionamiento:

- a) El cifrado debe poder ser integrado en la línea de comunicación sin tener que modificar el equipo de comunicaciones.
- b) Debe manejar un flujo de información full-duplex asincrónica serial, soportando las diferentes velocidades de transmisión que son de uso general.
- c) Debe permitir cambiar del método del cifrado de una manera simple.
- d) El proceso de cifrado/descifrado se debe hacer continuamente y en tiempo real, pues está fluyendo la información.

Para alcanzar la primera meta, los dispositivos fueron diseñados para ser integrados en cada lado del sistema de comunicación, se pueden colocar en los extremos de la línea de la transmisión, o se colocan como una interfaz entre el usuario y el equipo de comunicación. Dependiendo del uso en donde el cifrado será utilizado y de las características del equipo y del medio de transmisión será el lugar más conveniente para implementar el proceso de cifrado. La Figura (2) muestra un diagrama de bloques de cómo la integración del sistema de seguridad se puede emplear en un sistema de comunicación. El mecanismo que cifra debe contener

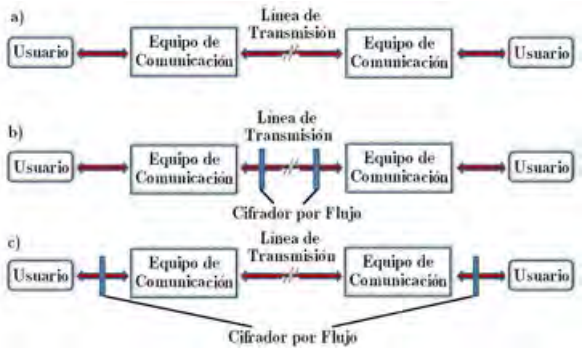


Figura 2. Diagrama de bloques de un sistema de comunicación simplificado. a) Sistema Inseguro. b) Sistema con el cifrado en los extremos de la línea de la transmisión. c) Sistema con el cifrado como interfaz entre el usuario y el equipo de comunicación.

generalmente un elemento central de control para realizar el proceso del cifrado/desciframiento, manejando y obteniendo la información a partir de dos interfaces en serie, según las indicaciones de la Figura (3). Para asegurarse de que el proceso

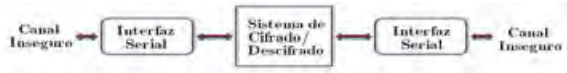


Figura 3. Diagrama de bloques del dispositivo de cifrado y Descifrado.

de cifrado/descifrado se realice continuamente sin afectar el flujo de información original, se decide trabajar con algoritmos de cifrado por flujo.

III. Diseño de la plataforma criptográfica

Para diseñar la plataforma criptográfica se inicia a partir de las especificaciones establecidas en la sección anterior. El método generalmente usado para intercambiar la información es la transmisión de datos serial o en serie, así se implementan dos puertos "Universal Asynchronous Receiver/Transmitter" (UART) para conectar la plataforma con el medio de comunicación, uno para recibir y enviar la información al usuario en el formato original, y el otro para recibir y enviar la información cifrada por el medio de transmisión. Esto permite integrar el proceso de cifrado en cualquier sistema de comunicación digital que utilice una transmisión de datos serial full-duplex asincrónica, sólo teniendo que desarrollar una interfaz para conectar el cifrador en el sistema de comunicación, dependiendo del lugar en donde será utilizado. Por otro lado para poner la plataforma criptográfica en ejecución se decide utilizar un FPGA, aprovechando sus características, incluyendo su operación de alta velocidad, bajo costo, facilidad de empleo y reconfiguración. En trabajo se decidió utilizar una tarjeta de desarrollo con un integrado XC3S500E, de la familia Spartan 3E de Xilinx. Este FPGA es de tamaño medio, con el equivalente a 500 mil compuertas lógicas. El integrado tiene gran capacidad de poder integrar la plataforma criptográfica junto con cualquier bloque que se quiera cifrar y evaluar. Esta plataforma de desarrollo funciona a 50 [MHz], que permite configurar el UART para funcionar a una velocidad de 3.125 [Mbps], que es bastante para funcionar en tiempo real como la mayor parte de los sistemas de comunicación. Ahora bien para probar la operación total del cifrador, que podría ser integrado en una línea de comunicación, primero se desarrolló el esquema de cifrado que se muestra en la Figura(4). Esta implementación consiste de un módulo con una máquina de estados que controle al dispositivo, maneje la operación de los UART y que lleve a cabo los procesos de cifrado y descifrado. Con este dispositivo, se prueba la plataforma

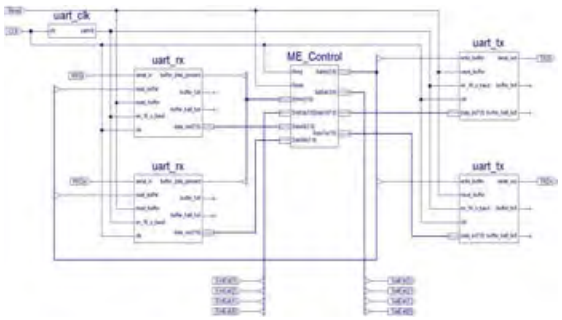


Figura 4. Diseño de la Plataforma integrando el bloque de control.

criptográfica y se utiliza para poner un proceso de cifrado en ejecución en un sistema de comunicación. En las pruebas de funcionamiento se colocaron dos de estos dispositivos entre dos PC que se comunican a través de un puerto serial RS-232. Los resultados de estas pruebas se presentan en la quinta sección de resultados. Con este diseño se puede verificar que la idea general funciona, pero esto no resuelve las características que se precisaron para la plataforma criptográfica, aquello de que debe ser fácil cambiar el algoritmo criptográfico usado. Esto es debido a que como se encaja dentro de la máquina de estados del control es necesario modificar el sistema entero para realizar un cambio simple. Por lo que se modifica este sistema para llevar al elemento de seguridad fuera de este control, colocando los procesos de cifrado/descifrado en un bloque separado, de modo que el bloque de control sea solamente responsable de manejar la comunicación a través de los UARTs, una vez que los datos sean procesados. Se toma la precaución para proveer al bloque de cifrado/descifrado los medios para que pueda trabajar con el bloque de control sin importar el algoritmo usado, de tal manera que la interfaz entre estos dos bloques sea tan general como sea posible y que

cuente con los mecanismos necesarios para alcanzar esto. Se define un protocolo simple de apretón de manos para informar al bloque de cifrado/descifrado cuando hay ciertos datos que se procesarán y posteriormente que de informe al bloque de control cuando han terminado los procesos, tomando cuidado de no perder información en el proceso evitando mandar más datos al bloque cifrador hasta que no haya terminado el proceso de los datos actuales. Al final, aunque el alcance

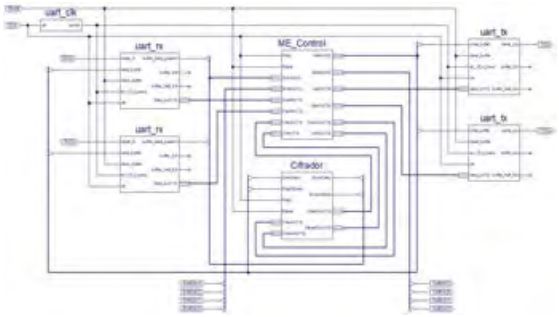


Figura 5. Diseño de la Plataforma Criptográfica incorporando el proceso de cifrado/descifrado como un bloque independiente.

de este trabajo está limitado al uso del $A5\_1$ en la plataforma de comunicación, el objetivo es tener un sistema de bloques de cifrado/descifrado con diversos algoritmos integrados, de modo que cuando se tiene que implementar un nuevo dispositivo que cifre/descifre, se desarrolle el bloque con el algoritmo deseado y se conecte con la plataforma para tener un sistema funcional. El dispositivo que resulta se puede observar en la Figura (5).

IV. Configuración de las Interfaces Seriales en la Spartan 3E

En esta sección se presenta la configuración que tienen las interfaces seriales en la tarjeta de desarrollo Starter Kit Spartan 3E de Xilinx, además de mostrar un esquema de conexión según la plataforma diseñada para realizar la comunicación serial segura. Los dos puertos serie que tiene la tarjeta Spartan 3E en la parte superior derecha, en realidad son dos conectores físicos DB9 denotados por DCE (hembra) y DTE (macho). El puerto estilo DCE se conecta directamente con el conector del puerto serial disponible en la mayoría de las computadoras personales vía un cable serial "*straight-through*" estándar. Un adaptador de géneros o cables cruzados no se requieren. Se usa el conector estilo DTE para controlar los otros periféricos RS-232, tales como módems o impresoras, o realice la prueba de "*loopback*" simple con el conector del DCE. La Figura (6) muestra la configuración de los pines para ambos estilos de conectores. El control de flujo del hardware no se apoya en el conectador. Las señales DCD, DTR, y DSR del puerto se conectan juntas, según se muestra en la figura. Similarmente, las señales RTS y CTS del puerto se conectan juntas. Se observan también los pines de conexión a la tarjeta Spartan 3E de acuerdo a las siguientes señales:

- $RS-232\_DCE\_RXD$ que corresponde al pin R7

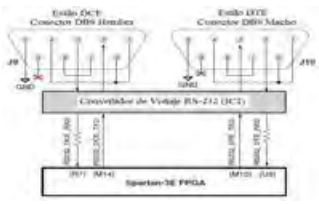


Figura 6. Puertos Seriales RS-232.

- $RS-232\_DCE\_TXD$ que corresponde al pin M14
- $RS-232\_DTE\_RXD$ que corresponde al pin U8
- $RS-232\_DTE\_TXD$ que corresponde al pin M13

A continuación se presenta el esquema para las conexiones usado de acuerdo a la plataforma criptográfica para la comunicación serial entre dos tarjetas Spartan 3E desarrollada, Figura (7).

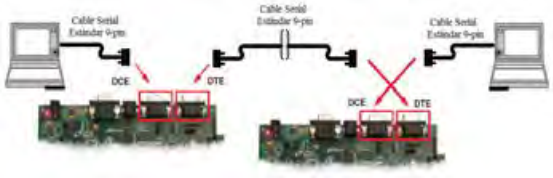


Figura 7. Esquema de conexiones para la plataforma criptográfica.

V. Resultados de la plataforma de comunicación

En esta sección se muestran las características obtenidas en la plataforma de comunicación serial durante su operación. Para probar la operación de la plataforma, primero se desarrollan bloques cifrados con algoritmos criptográficos simples, para medir el funcionamiento de la plataforma sin el efecto de la respuesta en tiempo de un bloque cifrado que resulta de un algoritmo criptográfico complejo. Esta es la razón del porqué para las primeras pruebas fueron realizadas usando César, Lucifer y otros algoritmos sencillos. Estos primeros cifradores fueron desarrollados originalmente dentro de la máquina de estados en el módulo de control de la Figura (5). Con esta clase de operación se encontró que el retardo total, incluyendo la lectura de un carácter desde la entrada del UART, el cifrado/descifrado del carácter y de escritura de ese carácter en la salida UART fue hecho de un máximo de 5 ciclos de reloj, como la tarjeta de desarrollo Spartan 3E trabaja a 50 [MHz], se tiene un tiempo total del proceso de 100 [nanosegundo]. Para establecer si este tiempo puede afectar al sistema de comunicación se debe comparar con el tiempo que toma para enviar un carácter como resultado de la velocidad de transmisión. Los puertos del UART que se utilizan en la plataforma necesitaron dividir la frecuencia de reloj por 16 para generar la frecuencia de transmisión de datos que garantiza una comunicación exacta. Consecuentemente se tiene 3.125 [Mbps] como velocidad máxima de transmisión. De esto se concluye que la plataforma puede funcionar correctamente sin afectar la velocidad de transmisión

del sistema original mientras el tiempo de proceso de datos total no exceda 16 ciclos de reloj. Desde este punto de vista, la plataforma resuelve completamente este requisito. Para probar la operación del cifrado se toma un sistema de comunicación que consiste en dos computadoras PC que se comunican a través de un puerto serial RS-232, poniendo un cifrador en cada extremo del cable de la conexión, según las indicaciones de la Figura (2b). Fue encontrado que la comunicación no fue alterada al enviar la información a cualquiera de las velocidades soportas por el puerto serial RS-232 de la PC, que incluye velocidades de hasta 115200 [bps]. Una vez que se validó la operación apropiada de la plataforma criptográfica, se hicieron las modificaciones apropiadas para extraer el algoritmo de cifrado del módulo de control y dejarlo como módulo externo que pude ser intercambiado fácilmente. El resultado de esta modificación se podría verificar dado que la plataforma criptográfica mantiene un desempeño similar que la versión anterior, solamente aumento en un ciclo de reloj el tiempo de reacción total, tomando 6 ciclos de reloj, que todavía está por debajo del sistema de límite de 16 ciclos de reloj dado por el UART. Entonces se evalúa el desempeño de la plataforma con un algoritmo más robusto, específicamente con el algoritmo A5_1 para cifrado de mensajes GSM (cifrador por flujo), que es más conveniente para la clase de aplicaciones que se desean implementar. La respuesta en tiempo que necesita el módulo que cifra y descifra depende del algoritmo de cifrado que en particular se utiliza. Se encontró que se tuvo que establecer un protocolo de apretón de manos para evitar soltar la información, esto es porque las señales de control fueron agregadas para informar al módulo de cifrado/descifrado cuando los datos están disponibles para ser procesados, y también informar al módulo de control cuando se termina el proceso de cifrado/descifrado. Lo cual dio lugar a un pequeño aumento en el tiempo de respuesta del sistema, dejando en 7 ciclos de reloj la respuesta total del tiempo, este aumento tiene que ser agregado al tiempo en que se cifra y descifra en el módulo cifrador. También deberá ser considerado cuando

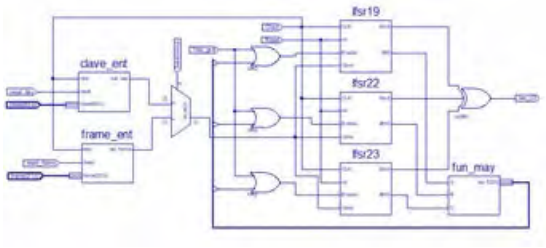


Figura 8. Implementación del algoritmo A5_1.

otras implementaciones de algoritmos tomen más tiempo para procesar los datos. La Figura (8) muestra la implementación del algoritmo $A5\_1$ mediante la construcción de los tres LFSR y la función de mayoría que se convierte en el bloque del cifrador en la plataforma criptográfica. En la Figura (9) se presenta el resumen de la implementación de algoritmo de cifrado que genera Xilinx de los recursos consumidos, en porcentajes.

Device Utilization Summary			
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Flip Flops	137	9,312	1%
Number of 4 input LUTs	193	9,312	2%
Number of occupied Slices	210	4,656	4%
Number of Slices containing only related logic	210	210	100%
Number of Slices containing unrelated logic	0	210	0%
Total Number of 4 input LUTs	194	9,312	2%
Number used as logic	187		
Number used as a route-thru	1		
Number used as Shift registers	6		
Number of bonded IOBs	93	232	40%
Number of BUFGMUXs	1	24	4%
Average Fanout of Non-Clock Nets	1.93		

Figura 9. Resumen del diseño del algoritmo A5_1 sobre la Spartan 3E.

VI. Conclusiones

Los resultados muestran la operación de la plataforma de comunicación vía un protocolo UART serial $RS-232$. Es claro que esta operación se efectúa sin ningun problema si se realiza la configuración adecuada y se tiene el equipamiento necesario para interconectar dos computadoras. La importancia de este desarrollo es que en la plataforma se puede intercambiar el bloque de cifrador por otro con las características tipo Verman y probar su eficencia y velocidad en el cifrado y descifrado de un mensaje. La relevancia decae en las implementaciones de cualquier algoritmo de cifrado en la plataforma con sus adecuaciones pertinentes o modos de operación y para aplicaciones en específico. Por lo mismo la plataforma puede ser utilizada bajo otros esquemas de protocolos de comunicación, por ejemplo las inalámbricas. Se programaron los FPGA de dos tarjetas Spartan 3E y se realizaron las pruebas mostrando los resumenes de ocupación sobre los chips xc3s500e-4fg320 de la Spartan 3E.

Agradecimientos

Este trabajo ha sido financiado por la Dirección General de Personal Académico de la Universidad Nacional Autónoma de México bajo el Programa de Apoyos para la Superación del Personal Académico a través de la beca doctoral.

Referencias

[1] Daltabuit E., Hernández L., Mallén G., Vázquez J., "La seguridad de la Información," Ed. Limusa, 2007.

[2] Prieto Meléndez R.,Padrón Godinez A., Herrera Becerra A.A., Calva Olmos V.G. *Generic Platform for the Implementation of Stream Ciphers in FPGAs.* 2nd ICIAS International Congress on Instrumentation and Applied Sciences, (2011).

[3] Martínez Reyes I., Padrón Godinez A., Prieto Meléndez R. Herrera Becerra A,A,. Calva Olmos V.G. *Generador de números pseudoaleatorios usando AES con modo contador: implementación en FPGA.* SOMI XXIX Congreso de Instrumentación, (2014).

[4] Padrón Godinez A., *Información cifrada en medios portadores*, Tesis de Maestría, ESIME-IPN (2013).

[5] Vázquez Sánchez J.A., Padrón Godinez A., Prieto Meléndez R. Herrera Becerra A,A,. Calva Olmos V.G. *Cifrador de flujo para tecnología GSM: una comparación entre hardware y software.* SOMI XXIX Congreso de Instrumentación, (2014).

[6] Prieto Meléndez R., Padrón Godinez A., Herrera Becerra A,A,. Calva Olmos V.G. *Implantación Electrónica de Cifradores de Flujo Tipo Vernam Utilizando Generadores Pseudoaleatorios.* SOMI XXVII Congreso de Instrumentación, (2012).

En búsqueda de polinomios primitivos para generación de secuencias mediante LFSR

1st Alejandro Padrón-Godínez
Instrum. Científica e Indus.
ICAT-UNAM
Cto. Ext. S/N, CDMX - México
alejandro.padron@icat.unam.mx

2nd Rafael Prieto Meléndez
Instrum. Científica e Indus.
ICAT-UNAM
Cto. Ext. S/N, CDMX - México
rafael.prieto@icat.unam.mx

3rd Victor Emmanuel Hernández López
Lab. Optica
Facultad de Ciencias - UNAM
Cto. Escolar S/N, CDMX - México
carlost@inaoep.mx

***Resumen*—En la solución de algoritmos eficientes en la generación de secuencias binarias mediante LFSR en cifradores de flujo se emplean polinomios primitivos para obtener los periodos máximos, que dependen del número de bits utilizados además de una semilla de bits diferente de cero. Algoritmos que tienen una complejidad polinomial en su solución, es decir el tiempo que tardan en correr y que crecen con el número de bits n en la entrada son de manera polinomial n^x con x ϵZ en una programación clásica. En el presente trabajo mostramos una búsqueda de polinomios primitivos para la obtención de los periodos máximos mediante un algoritmo clásico, la implementación en dispositivos de lógica programable en VHDL de un LFSR para la verificación de los periodos máximos y resultados preliminares en la solución del algoritmo mediante simulaciones en cómputo cuántico en la generación de secuencias binarias pseudoaleatorias.**

***Palabras Clave*—Cifradores de Flujo, Sistemas de Lógica Programable FPGA, Polinomios Primitivos.**

I. Introducción

La generación de secuencias binarias pseudoaleatorias generadas por sistemas de cómputo digitales han permitido que muchas aplicaciones tanto en software como en hardware puedan emplearse en algoritmos estándares de Criptografía. El manejo de la información clasificada o privada en forma segura es tan necesaria como la utilización de dispositivos modernos y actualizados. La velocidad de las comunicaciones en diversas transacciones nos anuncia el empleo de cifradores de flujo casi en tiempo real, ésta es la necesidad para que los algoritmos de cifrado deban ser optimizados ante los nuevos desarrollos tecnológicos y puedan evitarse ataques a los sistemas de información. Ya han sido anunciados y publicados los algoritmos poscuánticos que tratan de evitar que sean ciptoanalizados justamente ante el poder de cómputo con plataformas cuánticas. [1]. En el ámbito de la implementación usando algoritmos de cifrado por flujo se han podido crear algunas estructuras mediante registros lineales retroalimentados por desplazamiento "LFSR" (Linear Feedback Shift Register, por sus siglas en inglés), como Shrinking, Geffe, Beth - Piper, sincronizadas o no por mencionar algunas. Esto para disminuir la posibilidad de alterar, modificar, borrar información que pueda ser interceptada por personal no autorizado (Hacker) aunque siempre habrá intentos mal intencionados. Algunos de los primeros algoritmos de flujo ya han sido quebrantados, por los mismos desarrolladores o grupos de criptoanalistas para mostrar sus vulnerabilidades ante la nueva tecnología computacional, ejemplo de ellos son RC4, A5_1 y WPA. Aunque estos algoritmo han sido y fueron las raices para los nuevos algoritmos que en combinación con modos de operación y otros algoritmos inclusive de bloque que aumentan el nivel de seguridad como en el caso de WPA2 y WPA3 con claves de AES-256.

PASPA-DGAPA-UNAM beca de doctorado.

Los LFSR se han utilizado para aplicaciones en comunicasiones celulares GSM, aunque para estas implementaciones no se rigen por un estándar ya que estos algoritmos se han mostrado en cuestiones de enseñanza para generación de secuencias binarias mediante operaciones OR-exclusivas. Lo que inicialmente se necesita una estructura que debe consistir de número de bits, semilla o vector de inicio VI (diferente de cero) y polinomio primitivo para su funcionamiento. [2], Fig. (1).

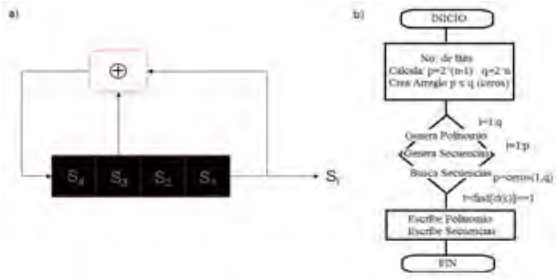


Figura 1. a) Diagrama de un LFSR de 4 bits con $P(x) = x^3 + x + 1$ y b) diagrama de flujo para el cálculo del polinomio primitivo y secuencias generadas.

La seguridad de los cifradores de flujo empleando polinomios primitivos de mayor orden aumenta, debido a que el periodo de las secuencias binarias obtenidas es mayor. Como se sabe el periodo máximo es el producto de cada periodo máximo empleado en el diseño de una configuración en particular. El diseño de nuevas configuraciones mediante LFSR, empleando polinomios primitivos, pueden ser más eficientes comparados con cifradores de flujo empleando modos de operación y cifradores de bloque. Lo cual puede analizarse en el tiempo de procesamiento de los criptogramas obtenidos,

por ejemplo un cifrador de bloque convertido en cifrador de flujo tiene que calcular las subclaves en cada iteración, en particular un “Output Feedback Block” con un AES-128.

En cuestiones de seguridad de la información se debe estar al tanto de que si se comprometen las claves secretas se compromete toda la seguridad de los sistemas protegidos. Por tal motivo hay que tomar en cuenta que la generació de claves, la distribución y el almacenamiento debe de efectuarse de forma segura. Sin embargo, el papel de contar con algoritmos de cifrado actualizados es primordial para proteger estos sistemas de información. Los algoritmos criptográficos modernos tendrán sus vulnerabilidades y podrán explotarse en cuanto se tenga acceso a plataformas modernas. Se podrá intentar criptoanalizar estos algoritmos, ya que con el uso de cómputo cuántico se trata de optimizar los algoritos clásicos para que procesen en menor tiempo. Un atacante que conoce el algoritmo puede intentar romper su seguridad y posiblemente tendrá a las manos las herramientas modernas, al mismo tiempo que se estén desarrollando los algoritmos postcuánticos. [3], [4].

Así empleando generadores de secuencias binarias pseudoaleatorios a partir de registros de desplazamiento retroalimentados lineales (LFSR por sus siglas en ingles) [5], se plantea la búsqueda de los polinomios primitivos de acuerdo al número de bits empleados, mediante un programa que prueba la combinación de polinomios hasta que se obtenga el periodo máximo. La razón de esta búsqueda de polinomios primitivos se debe a que en la literatura sólo se menciona que existen tablas donde se pueden encontrar estos generadores de secuencias y que no son de fácil acceso. Se pueden verificar si con los polinomios primitivos se obtienen los periodos máximos realizando las pruebas estadísticas publicadas por la NIST en la norma SP 800-22 para generadores secuencias pseudoaleatorias en aplicaciones criptográficas o simplemente usando los Postulados de Golomb incluidas como pruebas en la misma norma. En paralelo se desarrolla una implementación de un LFSR en Lenguaje de Descripción de Hardware (VHDL) sobre Sistemas de Logica Programable (FPGA) bajo la plataforma de desarrollo Xilinx, mostrando los resultados en una simulación para un número de bits, una semilla y de acuerdo al polinomio primitivo seleccionado.

En este trabajo también se muestra un desarrollo preliminar bajo la plataforma de Qiskit para bajo un modelo cuántico como puede generarse dada la densidad de probabilidad una secuencia binaria pseudoaleatoria en cada proceso. Planteando con esto si es posible implementar el algoritmo desarrollado para encontrar los polinomios primitivos de acuerdo al número de bits empleados para optimizar su cálculo. En las conclusiones mostraremos la problemática que se encontró cuando el número de bits aumenta y se mostrarán las perspectivas del trabajo. [6].

II. Características de los LFSR

Los LFSR han sido planteados como generadores de claves por varias razones, por ejemplo: son fáciles de implementar en hardware, producen secuencias con periodo grandes, producen secuencias binarias con buenas propiedades estadísticas y debido a su estructura pueden ser analizados con técnicas algebraicas [7]. Cuando se usan LFSR, la seguridad de los sistemas de comunicación depende mucho de que tan vulnerable sea el medio de transmisión y como puede verse afectado ante ataques pasivos y activos. En implementaciones reales como GSM, se encuentran algunas propiedades que deben cumplir dentro un sistema de seguridad de información para su buen funcionamiento:

- a) El cifrado debe poder ser integrado en la línea de comunicación sin tener que modificar el equipo de comunicaciones.
- b) Debe manejar un flujo de información full-duplex asincrónica serial, soportando las diferentes velocidades de transmisión que son de uso general.
- c) Debe permitir cambiar el número de bits a la entrada de una manera simple.
- d) El proceso de cifrado/descifrado se debe hacer continuamente y en tiempo real.

Si se quiere alcanzar la primer propiedad, los algoritmos dentro del sistema de información deben de ser diseñados para imlementarse en cada lado del sistema de comunicación, se pueden colocar en los extremos de la línea de la transmisión, o se colocan como una interfaz entre el usuario y el equipo de comunicación. Dependiendo del uso en donde el cifrado será utilizado y de las características del equipo y del medio de transmisión será el lugar más conveniente para implementar el proceso de cifrado. El proceso de los LFSR dependen de tres parámetros principales, polinomio generador, número de bits y semilla de acuerdo con el número de bits. La Figura (2) muestra como pueden ser los polinomios de los generadores de secuencias binarias. Estos polinomios pueden ser factori-

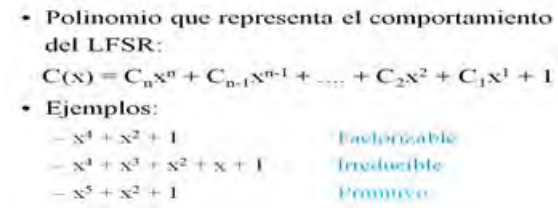


Figura 2. Polinomios para el diseño de LFSR que dictan las operaciones sobre los registros de desplazamiento por retroalimentación.

zables, irreducible y primitivos, para los cuales se buscan los polinomios primitivos que pueden generar el periodo máximo de acuerdo al número de bits empleados. Donde el periodo máximo se calcula como $T_{max} = 2^n - 1$, con n: No. de bits. La Figura (3) representa el diagrama de un LFSR para 8 bits. En el caso de que se utilicen polinomios que no son primitivos el periodo máximo no se alcanzará, la Figura(4) es un ejemplo de esto, para este LFSR de 4 bits se empleo una semilla “0111” y un polinomio generador $P(x) = x^4 + x^2 + 1$. Como se verán en los resultados sólo existen dos polinomios primitivos generadores del periodo máximo para 4 bits.

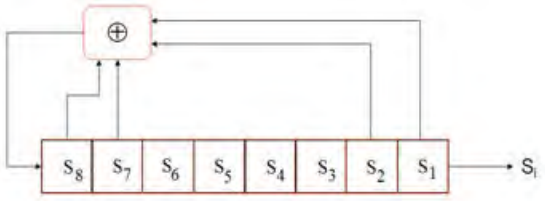


Figura 3. LFSR de 8 bits con operaciones xor para la retroalimentación según el polinomio primitivo $P(x) = x^8 + x^7 + x^2 + x + 1$.

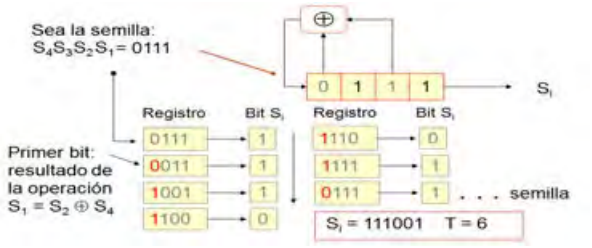


Figura 4. Polinomio que no genera las secuencias binarias del periodo máximo de un LFSR de 4 bits.

III. Estructuras de LFSR No Lineales

En la creación de estructuras no lineales usando LFSR se han construido varias estructuras donde se intenta aumentar el periodo de las secuencias binarias generadas, donde ahora el cálculo del periodo máximo es el producto del periodo máximo de cada LFSR contenido en la estructura. En la literatura se pueden encontrar algunas estructuras haciendo uso de LFSR en diferentes configuraciones que pueden ser síncronas o no sincronizadas. En la Figura(5) se muestra una primer distribución de LFSR conocida como generador Geffe. Una segunda estructura usando LFSR de diferentes tamaños se

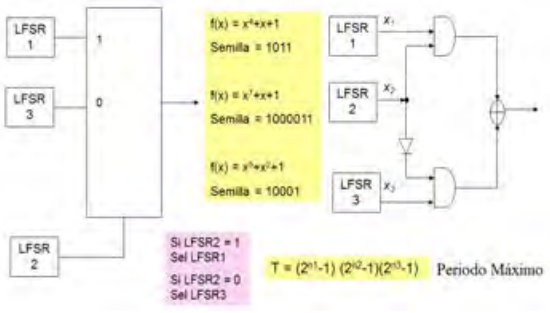


Figura 5. Diseño de un Generador Geffe de secuencias binarias.

ilustra en la Figura (6), denomida como generador Beth - Piper. Una tercer estructura al final de esta sección se presenta en la la Figura (7), que tiene el nombre de generador Shrinking. Hay muchos desarrollos de cifradores de flujo con diversas estructuras usando e implementando LFSR en su construcción que fueron las raices de las primeras aplicaciones como urnas electrónicas, tokens para control de acceso o en telefonía celula

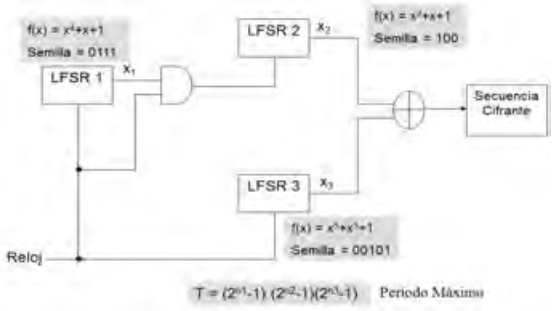


Figura 6. Estructura para un Generador Beth - Piper.

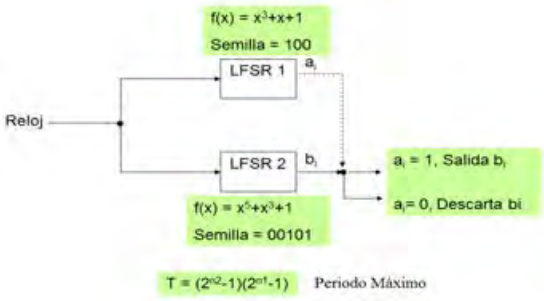


Figura 7. Configuración de un Generador Shrinking.

por mencionar algunas. Otras implementaciones contienen elementos adicionales como en el caso de los algoritmos $A5\_1$ y $A5\_2$ que emplean funciones de mayoría para variar los avances en cada paso de los LFSR en el proceso de envío de datos para cifrar y descifrar.

IV. Algoritmo de Grover modelo de computación cuántico

Para la computación cuántica el algoritmo de Grover es uno de los algoritmos de búsqueda, que permite realizarla en un espacio de $O(n^{1/2})$ en ves de $O(x^n)$ como los hacen los algoritmos clásicos. Este algoritmo permite realizar la búsqueda, mediante una densidad de probabilidad muy grande, un elemento de una secuencia no ordenada de una serie combinacional. El algoritmo de Grover tiene como meta encontrar un estado marcado ($|t\rangle$) en un conjunto desordenado, mostrado por un elemento en la base canónica. Emplea como estado inicial la superposición uniforme de todos los elementos $O(x^n)$ de la base computacional al que llamaremos $|s\rangle$. El algoritmo se basa en aplicar sucesivamente el operador $O = (2|t\rangle\langle t| - I_d)$ y el operador $G = (2|s\rangle\langle s| - I_d)$. El operador O ó G tiene como vector propio al vector $|t\rangle$ ó $|s\rangle$ asociado al valor propio 1. El resto de los vlores propios son -1 y corresponden a una base de vectores ortogonales a $|t\rangle$ ó $|s\rangle$. Por lo tanto el operador de Grover $U_g = G.O$ no es más que una reflexión sobre el subespacio generado por $|t\rangle$ y $|s\rangle$. Luego de aplicar $O(n^{1/2})$ iteraciones se obtiene un estado muy

cercano a $|t\rangle$. El algoritmo de Grover consiste de la iteración de las dos fases siguientes:

- Consulta
- Inversión sobre la media

Suponiendo que tenemos una lista de N componentes, en la que hay m elementos marcados, el algoritmo de Grover permite maximizar las amplitudes de los elementos marcados en un tiempo breve, lo que hace más fácil obtener un elemento marcado cuando se realiza la observación del sistema.

V. Resultados para el cáculo de número de Polinomio Primitivos

En esta sección se muestran los resultados obtenidos para la búsqueda de los polinomios primitivos generadores de los periodos máximos en LFSR de acuerdo al número de bits de entrada. Para lograr este objetivo se desarrollo un programa computacional que prueba las diferentes combinatorias por número de bits que dieran como resultado precisamente el periodo máximo. En el programa también se tuvo el cuidado de obtener el tiempo de proceso cuando el número de bis empieza a aumentar. En la Tabla (I) se presentan los resultados hasta 14 bits debido a que la capacidad para guardar las secuencias generadas se ve limitada al espacio de almacenamiento generando archivos de Megabytes y el tiempo de espera va creciendo exponencilmente con el aumento de bits en la entrada. Motivo suficiente para optimizar este desarrollo para que sea eficiente y de ser posible implementarlo mediante plataformas de cómputo cuántico.

Cuadro I
No. Polinomios Generadores del periodo máximo

No. de Bits	*No. Pol. Prim.*	*Tiempo [s]*
3	*2*	*0.024378*
4	*2*	*0.009135*
5	*6*	*0.029094*
6	*6*	*0.098124*
7	*18*	*0.374736*
8	*16*	*1.482539*
9	*48*	*6.514709*
10	*60*	*23.359722*
11	*176*	*95.106123*
12	*144*	*384.922147*
13	*630*	*1558.68514*
14	*756*	*6392.023456*

La Figura (8) muestra la gráfica de los resultados obtenidos, observándose que para valores mayores de bits en la entrada la tendencia en el tiempo es aumentar exponencialmente.

Analizando los resultados de la Tabla (I) y la Figura (8) se puede notar que el crecimiento en el número de polonomios generadores del periodo máximo no es contino o uniforme, en algunos casos aumenta y en un valor siguiente de bits en la entrada disminuye. Como en el caso entre 6, 7 y 8 bits de entrada y en 10, 11 y 12. En el caso de la columna del tiempo en la Tabla (I), estos valores siempre aumentan, ya que aunque el programa no se detiene hasta que prueba todas las posibles combinaciones 2^n de polinomios generadores.

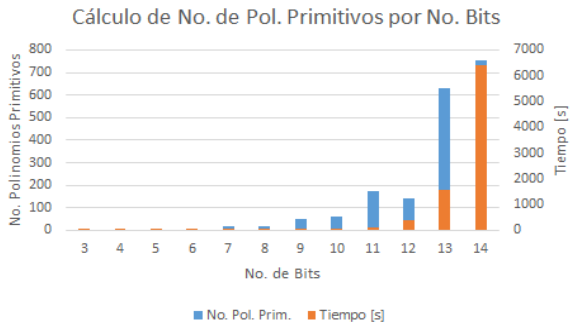


Figura 8. Resultados del cálculo de los Polinomios Primitivos por número de Bits y tiempo de procesamiento, datos de la Tabla (1).

Ahora se presentan los resultados para la implementación de un LFSR de 8 bits tomando el Polinomio Primitivo del renglón 98, que corresponde a $P(x) = x^8 + x^7 + x^2 + x + 1$. Polinomios Primitivos de 8 bits: (Iniciando con la potencia x^1 con el bit menos significativo)

- que corresponde al renglón 15 = [0 0 0 1 1 1 0 1]
- que corresponde al renglón 22 = [0 0 1 0 1 0 1 1]
- que corresponde al renglón 23 = [0 0 1 0 1 1 0 1]
- que corresponde al renglón 39 = [0 1 0 0 1 1 0 1]
- que corresponde al renglón 48 = [0 1 0 1 1 1 1 1]
- que corresponde al renglón 50 = [0 1 1 0 0 0 1 1]
- que corresponde al renglón 51 = [0 1 1 0 0 1 0 1]
- que corresponde al renglón 53 = [0 1 1 0 1 0 0 1]
- que corresponde al renglón 57 = [0 1 1 1 0 0 0 1]
- que corresponde al renglón 68 = [1 0 0 0 0 1 1 1]
- que corresponde al renglón 71 = [1 0 0 0 1 1 0 1]
- que corresponde al renglón 85 = [1 0 1 0 1 0 0 1]
- que corresponde al renglón 98 = [1 1 0 0 0 0 1 1]
- que corresponde al renglón 104 = [1 1 0 0 1 1 1 1]
- que corresponde al renglón 116 = [1 1 1 0 0 1 1 1]
- que corresponde al renglón 123 = [1 1 1 1 0 1 0 1]

— No. de polinomios primitivos calculados:16 —

La Figura (9) muestra la simulación en VHDL del LFSR de 8 bits que se seleccionó, donde se uso una semilla inicial igual a “10000001” en amarillo como vector de inicio. En la misma figura se muestran los primeros 10 periodos en gris o iteraciones del LFSR y los periodos donde se repite la semilla, no en 255 sino en 256 por la carga de la semilla en el inicio de los periodos, cuando el reset en verde se coloca en 1.

La secuencia binaria generada es:

Secuencia:(1 0 0 0 0 0 0 0 1 1 0 1 1 0 1 0 1 0 0 0 1 0 0 1 0 1 1 1 1 1 0 0 1 0 1 1 0 0 0 1 0 0 0 1 1 0 0 1 1 0 0 0 1 1 1 0 0 0 0 1 1 0 0 0 0 0 1 1 1 0 1 1 0 0 0 0 1 0 1 0 1 1 0 0 1 0 0 1 1 1 0 0 1 1 1 0 1 0 1 0 1 1 1 1 1 1 1 1 1 0 1 1 0 1 1 0 0 1 1 1 1 0 0 0 1 1 0 1 0 1 1 1 0 0 1 0 0 0 0 1 1 1 1 0 1 1 1 0 1 1 1 1 0 1 0 0 0 0 0 1 0 0 0 0 0 0 1 0 1 1 0 1 1 1 1 1 0 0 1 1 0 1 1 1 0 0 0 1 0 1 1 1 0 1 0 0 1 1 0 0 1 0 1 0 1 0 0 1 0 0 1 0 0 0 1 0 1 0 0 0 0 1 0 0 1 1 0 1 0 0 0 1 1 1 1 1 0 1 0 1 1 0 1 0 0 1 0 1 0 0 1 1 1 1 1 1).

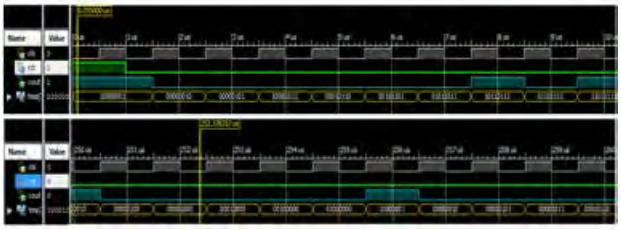


Figura 9. Simulación en ciclos de tiempo del LFSR de 8 bits seleccionado desarrollado en el simulador de la plataforma Xilinx.

Para este Polinomio Primitivo de grado ocho en particular se tienen los siguientes resultados cuando se realizan las pruebas estadísticas sobre la secuencia binaria generada [7].

- Tamaño de la secuencia = 255
- No. de ceros = 127
- No. de unos = 128
- La diferencia debe ser uno, 1er postulado,
- Que también es 1/2 de la secuencia para PG2a
- Dif.$0sy1s$ = 1
- ****Prueba de frecuencia****
- X1 = 0.0039
- ****Prueba de series o prueba de los 2-bit****
- Longitud 2 = 63 64 63 64
- Un 1/4 de la secuencia para PG2b
- X2 = 0.0118
- ****Prueba de póquer ****
- constantes m=3, k=85
- Longitud 3 = 31 32 31 32 31 32 32 32
- Que es 1/8 del tamaño de la secuencia para el PG2c
- X3 = 668.2235
- ****Prueba de rachas****
- NoBloques_Tam123 = 32 16 8, NoHuecos_Tam123 = 32 16 8
- ValoresD_e = 32.1250 16.0000 7.968 para calcular X4
- X4 = 0.0012
- ****Prueba de Autocorrelación con XOR y desplazamiento****
- X5 = -3.3883
- Para el 3er Postulado de Golomb
- Donde Xi son indicadores de las 5 pruebas

— Pruebas Estadísticas sobre la Secuencia Binaria —

Por último se presentan los resultados preliminares para optimizar el algoritmo utilizado con el cálculo de ceros y unos de un LFSR de 8 bits. La implementación práctica es de la siguiente manera, suponga que se tiene una función f tal que $f(x) = 1$ para los elementos marcados (conocidos). Se puede implementar un oráculo mediante un operador cuántico con ayuda de un qubit auxiliar. Si x es un estado cuántico de cualquier número de qubits y y el estado de un único qubit, se define a $U_f|x\rangle \otimes |y\rangle = |x\rangle \otimes |y\rangle \oplus f(x)$, donde $\oplus$ representa la operación XOR de dos bits. Si se usa $|y\rangle = |-\rangle = H|1\rangle$, se obtiene que $U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$, donde se nota que $f(x) = 1$ y se obtiene el cambio de signo en el estado $|x\rangle$. Se observa que en ningún momento se necesitó conocer explícitamente f para implementar U_f, y en general, esta función depende del problema en cuestión. Para la implementación práctica como la compuerta U_f depende fuertemente de la función f, y esta a su vez depende del problema en cuestión. Así se debe construir de manera que se adapte a los elementos marcados o conocidos. Para un ejemplo donde la lista de búsqueda es de $2^n - 1 = 255$ elementos con $n = 8$, de los cuales 16 elementos son marcados. Se necesitan un bit auxiliar por lo que se necesitarán 9 qubits. La implementación del operador U_f en kisquit se haría como:
def Uf(circuito, qreg)
circuito.ccx(qreg[0],qreg[1],qreg[2].qreg[3],qreg[4],
qreg[5].qreg[6],qreg[7],qreg[8])
Es decir, el tercer qubit es controlado por los dos primeros, pero ocurre un efecto interesante, como los dos primeros qubits se les aplica la compuerta H al aplicar el operador CNOT los qubits de control se ven afectados, en particular el elemento correspondiente al índice $|11111111\rangle$ sufre un cambio de signo, que es justo lo se busca, este fenómeno se conoce como phase kickback. Luego se implementa la inversión y se emplea la compuerta de Hadamard de 8X8 con entradas iguales a 0.5 y de -0.5 en la diagonal principal. Ahora se usan ambos operadores para implementar el algoritmo:

- Se crea un circuito con 9 qubits, donde 8 serán los que representan la lista y el último es el qubit auxiliar
- Se crea también 9 bits normales para almacenar las mediciones
- Se aplica H a los ocho primeros qubits para ponerlos en superposición
- Se lleva el qubit auxiliar al estado $|-\rangle$ para aplicar U_f
- Se aplica las fases de consulta e inversión las veces necesarias
- Se devuelve el qubit auxiliar a su estado inicial
- Se miden los resultados

En la Figura (10) se puede apreciar el circuito generado bajo la plataforma kisquit, en un inicio se observan 10000 veces el estado "11000011" el cual es el más observado al ejecutarlo una sola vez cada fase, que corresponde al elemento 98 seleccinado de la lista, que es el elemento marcado. Se puede

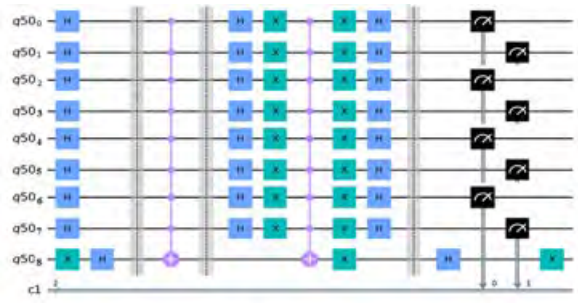


Figura 10. Modelo de Grover para 8 bits desarrollado en la plataforma cuántica Qiskit.

cambiar el número de iteraciones, por ejemplo dos iteraciones:

- renglón 15 = [0 0 0 1 1 1 0 1] 624 observado
- renglón 22 = [0 0 1 0 1 0 1 1] 626 observado
- renglón 23 = [0 0 1 0 1 1 0 1] 620 observado
- renglón 39 = [0 1 0 0 1 1 0 1] 622 observado
- renglón 48 = [0 1 0 1 1 1 1 1] 631 observado
- renglón 50 = [0 1 1 0 0 0 1 1] 627 observado
- renglón 51 = [0 1 1 0 0 1 0 1] 619 observado
- renglón 53 = [0 1 1 0 1 0 0 1] 617 observado
- renglón 57 = [0 1 1 1 0 0 0 1] 627 observado
- renglón 68 = [1 0 0 0 0 1 1 1] 621 observado
- renglón 71 = [1 0 0 0 1 1 0 1] 605 observado
- renglón 85 = [1 0 1 0 1 0 0 1] 629 observado
- renglón 98 = [1 1 0 0 0 0 1 1] 645 observado
- renglón 104 = [1 1 0 0 1 1 1 1] 633 observado
- renglón 116 = [1 1 1 0 0 1 1 1] 623 observado
- renglón 123 = [1 1 1 1 0 1 0 1] 630 observado

— No. de polinomios primitivos observados:16 —

Y así pueden seguirse calculando a través de más iteraciones, un detalle observado es que de acuerdo a las iteraciones en que se observa más el elemnto marcado son periódicas.

VI. Conclusiones

Los resultados muestran el número de polinomios primitivos generadores de secuencias binarias para el periodo máximo, de acuerdo al número de bits a la entrada de cada LFSR. Así como el tiempo que se tardo en obtener los polinomios, en realidad las potencias para cada polinomio primitivo. Se mostró la gráfica de los resultados para ver la tendencia exponencial cuando aumenta el número de bits a la entrada. Como se mencionó antes de la Tabla (I), el algoritmo de búsqueda debe optmizar tal vez hasta $2^{n/2}$ para reducir el espacio de almacenamiento y el tiempo para el cálculo, como en el caso del ataque por cumpleaños. Se presentó la simulación en VHDL para la verificación del periodo máximo en el caso particular de 8 bits en la entrada. Se hicieron pruebas estadísticas sobre las secuencias binarias producidas para este caso que se presentan en la literatura, desarrollando el programa para los Postulados de Golomb y las cinco pruebas de la referencia [7] para obtener los resultados mostrados. Se realizó las pruebas preliminares bajo la plataforma kisquit del modelo de Grover para encontrar secuencias binarias de ocho bits, en búsqueda de la optimización del algoritmo de búsqueda para encontrar las potencias de los polinimios primitivos aqui mostrados hasta 14 bits. Dado que el modelo de Grover realiza una búsqueda de un elemento en una secuencia no ordenada de 2^n en un espacio de $O(n^{1/2})$. Sin dejar de mencionar, que el archivo para los resultados de 14 bits en la entrada pesa 64,414 Kbytes.

Agradecimientos

Este trabajo ha sido financiado por la Dirección General de Personal Académico de la Universidad Nacional Autónoma de México bajo el Programa de Apoyos para la Superación del Personal Académico a través de la beca doctoral. En particular, un agradecimiento al Grupo Académico de Modelado y Simulación de Procesos del ICAT-UNAM, por el tiempo proporcionado en su equipo de 12 núcleos para el procesamiento de los cálculos en este trabajo presentados.

Referencias

[1] Daltabuit E., Hernández L., Mallén G., Vázquez J., “La seguridad de la Información,” Ed. Limusa, 2007.

[2] Prieto Meléndez R.,Padrón Godinez A., Herrera Becerra A.A., Calva Olmos V.G. *Generic Platform for the Implementation of Stream Ciphers in FPGAs.* 2nd ICIAS International Congress on Instrumentation and Applied Sciences, (2011).

[3] Martínez Reyes I., Padrón Godinez A., Prieto Meléndez R. Herrera Becerra A,A,. Calva Olmos V.G. *Generador de números pseudoaleatorios usando AES con modo contador: implementación en FPGA.* SOMI XXIX Congreso de Instrumentación, (2014).

[4] Padrón Godinez A., *Información cifrada en medios portadores*, Tesis de Maestría, ESIME-IPN (2013).

[5] Vázquez Sánchez J.A., Padrón Godinez A., Prieto Meléndez R. Herrera Becerra A,A,. Calva Olmos V.G. *Cifrador de flujo para tecnología GSM: una comparación entre hardware y software.* SOMI XXIX Congreso de Instrumentación, (2014).

[6] Prieto Meléndez R., Padrón Godinez A., Herrera Becerra A,A,. Calva Olmos V.G. *Implantación Electrónica de Cifradores de Flujo Tipo Vernam Utilizando Generadores Pseudoaleatorios.* SOMI XXVII Congreso de Instrumentación, (2012).

[7] Meneses J., Oorschot P., “Handbook of Applied Cryptography,” Ed. CRC Press Inc., 1997.

Cajas S: Una Visión General Acerca del Corazón de los Cifradores

David Carcaño Ventura
Coordinación de Ciencias Computacionales
Instituto Nacional De Astrofísica Óptica y Electrónica
Puebla, Mexico
carvendavid@gmail.com

Lil María Rodríguez Henríquez
Coordinación de Ciencias Computacionales
Instituto Nacional De Astrofísica Óptica y Electrónica
Puebla, Mexico
Consejo Nacional de Humanidades, Ciencias y Tecnologías
Mexico City, Mexico
lmrodriguez@inaoep.mx

Saúl E. Pomares Hernández
Coordinación de Ciencias Computacionales
Instituto Nacional De Astrofísica Óptica y Electrónica
Puebla, Mexico
CNRS, LAAS
Toulouse, France
spomares@inaoep.mx

***Abstract*—Las cajas S son consideradas el corazón de los cifradores de llave simétrica debido a la no-linealidad que ofrecen. Estas cajas S son funciones booleanas con un trasfondo matemático complejo, lo que en ocasiones dificulta la comprensión de los conceptos, convirtiendo en un desafío profundizar en el tema. Por ello, este trabajo presenta una visión general sobre lo que es una caja S, explicando sus métricas de seguridad y mostrando el trabajo que actualmente está en desarrollo. De esta manera, este artículo pretende crear una motivación al lector para que se continúe explorando este tema.**

***Index Terms*—Cajas S, Cifradores, AES, Ataque Diferencial, Propiedades de la Caja S.**

I. Introducción

Las cajas S son funciones booleanas que se han estudiado por más de 30 años debido a la seguridad que pueden ofrecer en los cifradores de llave simétrica. Éstas, consideradas como el corazón de los cifradores, son el principal componente para proveer el servicio de confidencialidad en la transmisión de datos [1], [2].

La caja S del cifrador AES [1] (siglas de Advanced Encryption Standard) [3] es una de las más utlizadas y estudiadas por la resistencia que ofrece ante los ataques criptográficos. Sin embargo, es suceptible a los ataques algebraicos debido a su construcción [4], y no siempre es la mejor opción para los cifradores ligeros [1]. Por lo que, en la actualidad se siguen buscando cajas S que puedan lograr un alto nivel de seguridad, utilizando un enfoque diferente de construcción y/o usando menos recursos de los dispositivos.

La búsqueda de nuevas cajas S es un desafío debido al inmenso espacio de búsqueda que existe y al complejo transfondo matemático. Por esta razón, se presenta una visión general sobre estas funciones de manera amigable, con el objetivo de que este trabajo sirva como referencia para introducir al novedoso tema sobre las cajas S.

[1]AES es un cifrador estandarizado por el NIST (siglas de National Institute of Standards and Technology) desde el 2001.

El artículo se organiza de la siguiente manera. En la sección II se muestra como funciona un cifrador de llave simétrica y el secreto para lograr la seguridad en las comunicaciones. La sección III define y explica la definición formal de la caja S. La sección IV presenta las diferentes representaciones de la caja S. En la sección V, se expone como obtener el nivel de seguridad de una caja S y se ejemplifica el caso del ataque diferencial. La sección VI muestra el trabajo actual sobre las cajas S. Y por último, la seccion VII presenta la conclusión de este trabajo.

II. El secreto de la seguridad en las comunicaciones

Los cifradores son una primitiva criptográfica usada para transmitir información confidencial entre dos o más entidades (personas, computadoras, robots, etc.). La figura 1 muestra como Alicia le envia un mensaje cifrado a Bob a través de un canal inseguro de comunicación. A pesar de que el adversario puede interceptar el mensaje cifrado Msj_C, éste no podrá conocer el mensaje original.

Para lograr esto, ambas entidades necesitan una llave sk. Ésta es secreta y solo las entidades de confianza deben tenerla (en este caso Alicia y Bob). Con esta llave, Alicia cifra el mensaje original Msj (también conocido como texto en claro) usando el cifrador C, y obtiene un mensaje cifrado Msj_C. Bob recibe Msj_C y recupera el mensaje original Msj usando la inversa del cifrador C^{-1} (también conocido como descifrador) y la llave sk.

Como se ha mencionado, el adversario puede interceptar el mensaje cifrado, ya que el canal de comunicación es inseguro. Sin embargo, el adversario no podrá descifrar el mensaje ya que no tiene la llave secreta. Además, aunque el adversario use un ataque de fuerza bruta, podría tomarle decadas encontrar la llave secreta [5].

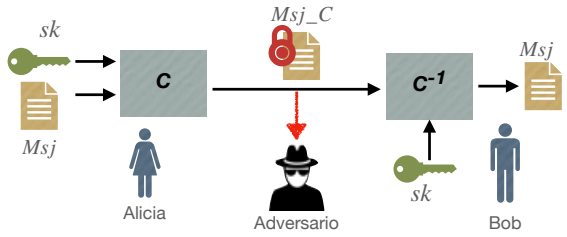


Fig. 1. Transmisión segura de datos entre Alice y Bob usando el cifrador C y la llave secreta sk.

A. Confusión y Difusión

Shannon estableció que un cifrador debe de cumplir con dos principios llamados confusión y difusión para garantizar la confidencialidad en el envío de información [6]. El principio de confusión establece que se debe romper la relación de la llave secreta con el texto cifrado. Mientras que el principio de difusión propone que se debe romper la estrucura estadística del texto en claro. Es decir, que si un bit del texto en claro cambia, al menos la mitad de los bits del texto cifrado también deben cambiar

Estos principios rompen las relaciones entre el texto en claro y el texto cifrado, así como entre la llave secreta y el texto cifrado, de tal forma que el adversario no pueda encontrar patrones para romper la seguridad del cifrador

Diferentes cifradores como AES [3], TWINE [7], ASCON [8] y CLEFIA [9] son usados para brindar seguridad en las comunicaciones. Para ofrecer los principios mencionados, estos cifradores utilizan cajas S (cajas de sustitución).

Las cajas S son funciones no lineales que actúan como los componentes principales en los cifradores, generando textos cifrados incomprensibles para el adversario. En la figura 2, se puede observar este efecto al cifrar el texto en claro $Msj\_Secreto = 128$ utilizando AES-128 y la llave secreta $0123456789abcdef$. Por esta razón, las cajas S son consideradas como el corazón de los cifradores.

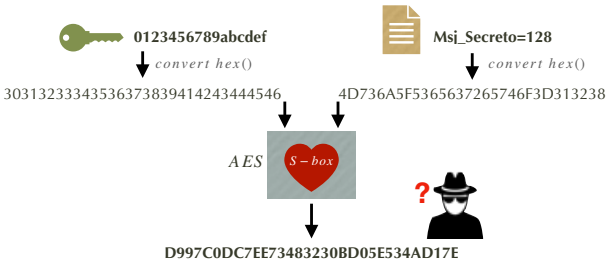


Fig. 2. Funcionamiento del cifrador AES.

III. ¿Qué es una caja S?

La caja S de un cifrador sustituye los bits del estado del cifrador. Esta caja recibe n bits de entrada y devuelve m bits de salida. Una definición más formal se presenta en [2], y es la siguiente:

Definición 1: Una caja S de tamaño $n \times m$ es una función booleana vectorial que sustituye un vector de dimensión n a un vector de dimensión m y se denota de la siguiente manera: $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$, donde n, m son enteros positivos y $\mathbb{F}_2^n$ es un vector de dimensión n en el espacio $\mathbb{F}_2$.

Daemen y Rijmen, los creadores de AES, diseñaron una caja S de tamaño $n = m = 8$ con el enfoque de construcción algebraico usando la función inversa X^{-1}, donde X representa los 8 bits de entrada. Esta caja se puede ver de la siguiente manera:

$$S(X) = (x^6+x^5+x+1)+X^{-1}\cdot(x^7+x^6+x^5+x^4+1)\ mod(x^8+1) \quad (1)$$

Debido a la seguridad que puede ofrecer, esta caja S sirve como referencia para el diseño de nuevas funciones no lineales. Esta función, que utiliza operaciones con polinomios, es el elemento clave más importante del cifrador AES. Dado que este cifrador es uno de los más utilizados, su caja S se ha convertido en el secreto para garantizar la seguridad de las comunicaciones [2], [3].

IV. Representaciones de la caja S

Las representaciones de la caja S ayudan a la visualización de este componente, así como su implementación en software y hardware, y permiten conocer el nivel de seguridad de la misma. En esta sección hablaremos de dos: LUT (siglas de Look Up Table) y ANF (siglas de Algebraic Normal Form).

Por convenencia de espacio, ejemplificaremos estas representaciones con la caja del cifrador TWINE. Esta caja emplea la misma construcción que AES (enfoque algebraico con la función inversa), pero usa un tamaño menor el cual es $n = m = 4$. Sin embargo, el lector se puede referir a [10] donde Bao et al. muestran la LUT y la ANF de la caja S de AES usando su herramienta PEIGEN [2].

A. Look Up Table (LUT)

Esta representación muestra todos valores de entrada y su respectiva salida en una tabla (o matriz). Las dos primeras columnas de la tabla I muestra la LUT de la caja de TWINE.

Existen diversas ventajas al emplear esta representación, entre las cuales se destacan las siguientes:

1) Visualización: La LUT de una caja S permite visualizar los valores de entrada y sus correspondientes sustitutos (valores de salida), sin necesidad de realizar los cálculos de la función.
2) Implementación: Cuando se implementa una caja en software, se utiliza la LUT de la caja para crear una matriz y almacenar los datos en memoria. De esta manera, cuando el cifrador necesita la caja, no emplea recursos en computar este componente, si no que solo busca los valores correspondientes en la matriz y los sutituye en el estado del cifrador [1].

LUT		Boolean functions			
X	$S(X)$	$\mathbb{B}_4(X)$	$\mathbb{B}_3(X)$	$\mathbb{B}_2(X)$	$\mathbb{B}_1(X)$
0	C	1	1	0	0
1	0	0	0	0	0
2	F	1	1	1	1
3	A	1	0	1	0
4	2	0	0	1	0
5	B	1	0	1	1
6	9	1	0	0	1
7	5	0	1	0	1
8	8	1	0	0	0
9	3	0	0	1	1
A	D	1	1	0	1
B	7	0	1	1	1
C	1	0	0	0	1
D	E	1	1	1	0
E	6	0	1	1	0
F	4	0	1	0	0

TABLA I
LUT DE LA CAJA S DE TWINE Y SUS FUNCIONES BOOLEANAS

3) Nivel de seguridad de la caja: La LUT permite analizar la caja S para conocer su resistencia ante ataques criptográficos como los diferenciales.

B. Algebraic Normal Form (ANF)

Las cajas S de tamaño $n \times m$ son funciones booleanas vectoriales. Sin embargo, estas cajas pueden ser la unión de m funciones booleanas. Por tanto, se presenta la siguiente definición:

Definición 2: Una función Booleana relaciona un vector de dimensión n a un elemento que pertenece a $\mathbb{F}_2$. En otras palabras la función lleva al vector de dimensión n a 1 o 0, y se denota de la siguiente manera $\mathbb{B}_n : \mathbb{F}_2^n \to \mathbb{F}_2$

La tabla I muestra la LUT de la función vectorial de la caja de TWINE y sus 4 funciones Booleanas. Se puede observar que la unión de las cuatro funciones $B_i(X)$ es la representación binaria de la salida hexadecimal $S(X)$. Esta conversión ayudará a enteneder la representación ANF de una caja S.

La ANF es una forma de representar cada función booleana de la caja S como el producto y sumatoria de sus entradas. Es decir, si tenemos m salidas, entonces tendremos m representaciones ANF de la caja, las cuales se llamaran coordenadas.

Las siguientes funciones Booleanas representan la ANF de las coordenadas de la caja de TWINE, donde X representa los cuatro bits de entrada $X = \{x_3, x_2, x_1, x_0\}$:

$$\mathbb{B}_1(X) = x_1 + x_0x_1 + x_0x_2 + x_0x_3 + x_2x_3 + x_0x_2x_3 \quad (1)$$

$$\mathbb{B}_2(X) = x_1 + x_2 + x_0x_3 + x_1x_3 + x_2x_3 + x_1x_2x_3 \quad (2)$$

$$\mathbb{B}_3(X) = 1 + x_0 + x_2 + x_3 + x_0x_2 + x_0x_3 + x_1x_3 + x_2x_3 + x_0x_1x_2 \quad (3)$$

$$\mathbb{B}_4(X) = 1 + x_0 + x_2 + x_0x_1 + x_1x_2 + x_0x_1x_2 + x_0x_1x_3 + x_1x_2x_3 \quad (4)$$

Es posible notar que en la tabla I, X representa los 4 bits de entrada de la caja. Por lo que si calculamos cada una de las funciones (1),(2),(3), y (4), usando los bits de entrada, podremos encontrar las salidas de $\mathbb{B}_1, \mathbb{B}_2, \mathbb{B}_3$, y $\mathbb{B}_4$ respectivamente.

Las ventajas de esta representación son:

1) Visualización: Observar la forma algebraica de la caja S.
2) Implementación: Las implementaciones de la caja S en hardware requieren calcular la función cada vez que el cifrador lo necesite, con el objetivo de no ocupar la memoria del dispositivo. Usando la ANF de la caja se pueden crear operaciones tipo Bit-slice para computar la salida de la caja cada vez que el cifrador lo requiera [11], [12].
3) Nivel de seguridad de la caja: Usando esta representación, se puede evaluar el nivel de seguridad de la caja ante ataques algebraicos.

Existen otro tipo de representaciones como la polar, pero las representaciones LUT y ANF son las más utilizadas en el estudio de cajas S.

V. NIVEL DE SEGURIDAD DE LA CAJA S

Al ser la caja S el corazón de los cifradores, ésta se ha convertido en el primer objetivo de los adversarios para vulnerar el cifrador usando los ataques *shrortcut* [13]. Estos ataques son más agresivos que los de fuerza bruta, ya que pueden reducir el trabajo computacional considerablemente para encontrar la llave secreta del cifrador.

Estos ataques se componen de dos fases:

1) El adversario intenta obtener distintivos analizando la caja S y encontrando patrones. Un distintivo es una característica que lleva información sobre la llave cuando es procesada por las rondas de un cifrador [14], [15].
2) Usando los distintivos obtenidos en la fase anterior, junto con parejas de textos en claros, y sus correspondientes textos cifrados, el adversario puede recuperar algunos o todos los bits de la llave secreta.

La caja S es fundamental para que el adversario no encuentre distintivos en el cifrador. Por ello, esta función debe ser lo más segura posible, pero ¿cómo podemos medir la seguridad de la caja?. La caja S tiene propiedades que permiten saber la resistencia ante ataques criptográficos. Estas propiedades ayudan a adversarios y diseñadores. Si los valores de las propiedades están alejados de lo óptimo, entonces el adversario puede vulnerar la caja para encontrar distintivos. En el mismo caso, pero para el diseñador, estos valores le permiten incrementar el nivel de seguridad del cifrador mediante el diseño de otra caja, para mejorar estos defectos y presentar una función más resistente.

La tabla II muestra algunos ataques y las propiedades a las que están relacionadas. En esta tabla se puede observar que un solo ataque puede estar asociada a muchas propiedades. Así pues, si se desea que una caja sea resistente a un ataque, el diseñador debería tomar en cuenta todas las propiedades relacionadas a ese ataque. Lograr lo óptimo en una sola propiedad no muestra la resistencia completa al ataque.

Ataque	Propiedad
Diferencial	Uniformidad diferencial (DU) Balance (B) CarD1
Lineal	Linealidad (L) CarL1 No-linealidad
Algebraico	Grado algebraico (AD) Minimo grado algebraico (MAE) Inmunidad algebraica (IA) Inmunidad algebraica de un grafo (GAI)

TABLA II
RELACIÓN DE LOS ATAQUES CRIPTOGRÁFICOS CON LAS PROPIEDADES DE LA CAJA S. LAS DEFINICIONES FORMALES DE ESTAS PROPIEDADES PUEDEN SER ENCONTRADAS EN DIFERENTES ARTÍCULOS INCLUYENDO [2], [16]–[18].

A continuación, se explicará el funcionamiento general de los ataques diferenciales y como podemos obtener una propiedad relacionada a este tipo de ataque, conocida como uniformidad diferencial.

A. *Resistencia de la caja S a los ataques diferenciales*

La figura 3 muestra como se realiza un ataque diferencial a un cifrador C en tres pasos. En el primer paso, se observa como el adversario elige un texto en claro P_1 y dos constantes a, b. Luego crea un segundo texto en claro P_2 computando la operación $P_1 \oplus a$. P_1, P_2 son dos textos en plano con una diferencia a. En el segundo paso, el adversario cifra los dos textos en plano P_1, P_2 y obtiene C_1, C_2 respectivamente. En el tercer paso, el adversario compara la diferencia de $C_1 \oplus C_2$ con respecto a la constante b. Si la comparación es correcta, entonces el adversario empieza a encontrar patrones para crear los distintivos. El objetivo de los ataques diferenciales es encontrar patrones cuando se analizan diferencias de textos en claro y sus respectivas salidas.

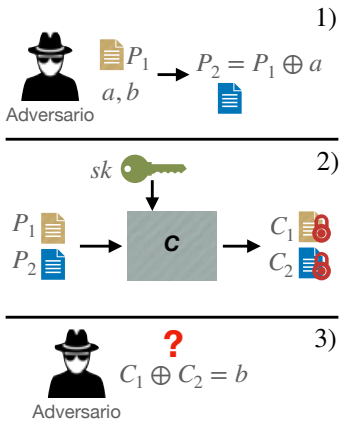


Fig. 3. Ataque diferencial a un cifrador C.

El ataque diferencial es uno de los más poderosos debido a que:

1) Puede reducir el factor de trabajo para encontrar la llave secreta. En [15], Stamp y Low muestran como se puede reducir el factor de trabajo a la mitad, en comparación a los de fuerza bruta, para encontrar la llave secreta del cifrador FEAL.
2) En [19], Shamir y Biham demuestran cómo encontrar distintivos diferenciales en todas las rondas del cifrador DES, a pesar de que sus cajas S presentan una alta resistencia frente a este tipo de ataque.
3) En la literatura, el diseño de cifradores que usan este tipo de función no lineal (tipo esponja [8], de flujo [20], caóticos [21], de bloque [14]) contemplan el ataque diferencial para evaluar la seguridad del cifrador y de la caja S.

Tomando como base el trabajo de Shamir y Biham en [19], a pesar de que el cifrador presente las cajas S con la más alta resistencia ante los ataques criptográficos, aún puede ser vulnerado. Sin embargo, esto debe de servir como motivación para seguir buscando cajas S que alcancen siempre el mejor nivel de seguridad, ya que si éstas presentan una vulnerabilidad, recuperar la llave será más sencillo.

En la literatura, el diseño de cajas S contemplan diversas propiedades relacionadas a este tipo de ataque entre ellas uniformidad diferencial, balance y CarD1. Este trabajo explica la uniformidad diferencial [22] que se obtiene usando una herramienta llamada DDT (siglas de Distribution Differential Table) [23]. Esta herramienta usa la LUT de la caja y se define de la siguiente manera:

Definición 3: DDT: Sea una caja S y dos vectores $a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2^m$, la DDT de S es una tabla de tamaño $2^n \times 2^m$ donde cada celda contiene el número de parejas a, b que cumplen la siguiente ecuación:

$$DDT_S(a,b) = |x \in \mathbb{F}_2^n : S(x) \oplus S(x \oplus a) = b| \qquad (2)$$

Cada celda de esta tabla refleja el número de veces que se cumple la ecuación (2) cuando se le da un valor a los vectores a y b. Se debe contemplar que x representa todos los datos de entrada de la caja S. En otras palabras, si consideramos $x = 8$ con la LUT de la caja S de TWINE, y elegimos los valores de $a = 5 = 0101$ y $b = 6 = 1010$ tendremos que verificar la siguiente igualdad:

$$\begin{aligned} S(8) \oplus S(8 \oplus 5) &= 6 \\ S(1000) \oplus S(1000 \oplus 0101) &= 0110 \\ 1000 \oplus S(1101) &= 0110 \\ 1000 \oplus 1110 &= 0110 \\ 0110 &= 0110 \\ 6 &= 6 \end{aligned}$$

Se puede notar que al resolver la ecuación, se cumple la igualdad. Si la ecuación se cumple, entonces el contador de $DDT(a,b)$ (la celda de este ejemplo $DDT(5,6)$) incrementa en uno. Ahora, si se quiere obtener el número de ecuaciones que cumplen la igualdad (2) cuando $a = 5$ y $b = 6$, se necesita resolver todas las ecuaciones cuando x toma el valor de todas las entradas de la caja S. Sin embargo, ya existen programas

DDT	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	2	0	0	2	0	0	0	2	2	2	4	0	0	2
2	0	0	0	2	2	2	0	2	0	0	4	2	0	0	2	0
3	0	0	2	0	0	2	2	2	2	0	0	0	0	0	2	4
4	0	0	0	2	0	0	2	0	0	2	0	4	0	2	2	2
5	0	2	4	2	0	0	2	2	0	2	2	0	0	0	0	0
6	0	2	0	0	0	4	0	2	0	2	0	0	2	2	2	0
7	0	0	0	2	2	2	2	0	2	4	0	0	2	0	0	0
8	0	2	2	4	2	2	0	0	0	0	0	0	0	2	0	2
9	0	0	0	2	0	0	0	2	4	0	2	0	2	2	0	2
A	0	2	0	0	2	0	0	4	2	2	0	2	0	0	0	2
B	0	0	2	0	2	0	2	2	0	0	0	2	2	4	0	0
C	0	0	2	0	2	0	0	0	2	2	2	0	0	2	4	0
D	0	4	2	2	0	0	0	0	2	0	0	2	2	0	2	0
E	0	2	0	0	4	0	2	0	0	0	2	0	2	0	2	2
F	0	2	0	0	0	2	4	0	2	0	2	2	0	2	0	0

TABLA III
DDT DE LA CAJA DE TWINE.

como PEIGEN [2] o SAGE [24], los cuales evaluan la caja y presentan el valor de todas las celdas de DDT. La tabla III muestra la DDT de la caja de TWINE.

Si las celdas de la DDT presentan valores altos, significa que la caja es más propensa a mostrar características diferenciales. En otras palabras, se puede vulnerar la caja para encontrar los distitivos de la primer fase del ataque. Por lo tanto, se presenta la siguiente definición:

Definición 4: DU (siglas de distribution uniformity): Es el valor más grande de la DDT donde $a \neq 0$ y se denota como:

$$DU(S) = \max_{a \neq 0}(DDT_S(a, b)) \tag{3}$$

Este valor debe ser lo más pequeño posible para que las cajas presenten la mayor seguridad ante este tipo de ataques. El DU que logra la caja de TWINE es 4 y es el valor más pequeño que se puede lograr cuando $n = 4$ (en otras palabras se considera el valor óptimo en ese caso).

VI. Trabajo a desarrollar sobre las cajas S

El objetivo principal de este tema es la búsqueda de nuevas funciones con alta resistencia a los ataques criptográficos. Sin embargo, ésto se divide en diversas líneas de investigación; aquí presentaremos tres: los compromisos entre las propiedades, las cajas S para cifradores ligeros y los enfoques de construcción

A. Compromisos entre las propiedades

La búsqueda de nuevas cajas S implica considerar que existen conflictos entre las mismas propiedades; al lograr lo óptimo en una, se puede alterar el nivel de seguridad de otra. En consecuencia, el diseñador debe establecer compromisos para lograr un equilibrio en el nivel de seguridad de esta caja. Algunos de estos conflictos son los siguientes:

1) Balance vs no linealidad [2]: Se ha demostrado que cajas la mejor no linealidad no pueden ser balanceadas.
2) CarL1 vs uniformidad diferencial [25]: CarL1 es una propiedad para cifradores con una capa de permutación de bit. Esta propiedad es importante para lograr la difusión. Sin embargo, el mejor valor que presenta esta propiedad cuando $n = m = 4$ (CarL1=1) ocasiona que la uniformidad no logre el valor óptimo (que es 4).

Debido a los diferentes conflictos, algunos trabajos buscan mejorar algunas propiedades de la caja S mientras analizan otras propiedades que se pueden alterar [26]. A su vez, se buscan proponer nuevos compromisos para tratar de lograr un nivel de seguridad balanceado entre las propiedades [17], [27].

B. Cajas S para cifradores ligeros

Un cifrador ligero está orientado a ser implementado en dispositivos que tienen recursos limitados, tales como los dispositivos IoT [1]. Este tipo de cifradores requieren que la caja sea de un tamaño más pequeño, en otras palabras una caja se considera ligera si $3 \leq n, m \leq 8$. Una caja más pequeña ocupara menos recursos del dispositivo para proveer los principios de confusión y difusión. No obstante, ésta no logrará el mismo nivel de seguridad que las cajas grandes. Por lo tanto, la búsqueda de cajas ligeras sigue siendo un problema en donde se debe considerar el compromiso entre la seguridad y el costo [28].

C. Enfoques de construcción

Existen diversos enfoques de construcción para la caja como el algebraico [3], heurístico [26] y la búsqueda aleatoria [9]. A pesar de que el enfoque algebraico ha logrado encontrar las mejores cajas debido a la alta resitencia que presentan ante los ataques ataques criptográficos, este tipo de construcción revela ser suceptible ante los ataques algebraicos [4]. Con base a esto, la mejora y la propuesta de nuevos enfoques de construcción es necesaria para cubrir esta vulnerabilidad.

VII. Conclusión

Las cajas S son muy importantes para proveer la confusión y difusión en los cifradores. Este trabajo presenta de forma general la importancia de esta función para crear los mensajes cifrados, la definición de este componente, la relación entre ataques y propiedades, y su nivel de seguridad. A su vez, se muestra algunos de los problemas actuales relacionados a la búsqueda de una caja S como la propuesta de compromisos entre las propiedades y el diseño de cajas S para cifradores ligeros.

El estudio de estas cajas conlleva una complejidad matemática que puede resultar desafiante para entender los conceptos relacionados con el tema. Por consiguiente, este trabajo busca servir como una referencia accesible para el lector, de modo que pueda profundizar en el estudio de este tema.

Referencias

[1] G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou, and C. Manifavas, "A review of lightweight block ciphers," *Journal of cryptographic Engineering*, vol. 8, pp. 141–184, 2018.
[2] Z. Bao, J. Guo, S. Ling, and Y. Sasaki, "Sok: Peigen – a platform for evaluation, implementation, and generation of s-boxes." Cryptology ePrint Archive, Paper 2019/209, 2019. https://eprint.iacr.org/2019/209.
[3] J. Daemen and V. Rijmen, *AES proposal: Rijndael*. Gaithersburg, MD, USA, 1999.

[4] N. T. Courtois and J. Pieprzyk, "Cryptanalysis of block ciphers with overdefined systems of equations," in *Advances in Cryptology—ASIACRYPT 2002: 8th International Conference on the Theory and Application of Cryptology and Information Security Queenstown, New Zealand, December 1–5, 2002 Proceedings 8*, pp. 267–287, Springer, 2002.
[5] C. Paar and J. Pelzl, *Understanding cryptography*, vol. 1. Springer, 2010.
[6] C. E. Shannon, "Communication theory of secrecy systems," *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.
[7] T. Suzaki, K. Minematsu, S. Morioka, and E. Kobayashi, "Twine: A lightweight, versatile block cipher," in *ECRYPT workshop on lightweight cryptography*, vol. 2011, Springer Berlin, Heidelberg, 2011.
[8] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon v1. 2: Lightweight authenticated encryption and hashing," *Journal of Cryptology*, vol. 34, pp. 1–42, 2021.
[9] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, "The 128-bit blockcipher clefia," in *Fast Software Encryption: 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers 14*, pp. 181–195, Springer, 2007.
[10] Z. Bao, J. Guo, S. Ling, and Y. Sasaki, "Peigen – a platform for evaluation, implementation, and generation of s-boxes," 2019. Accessed: September 27, 2024.
[11] L. Li, J. Liu, Y. Guo, and B. Liu, "A new s-box construction method meeting strict avalanche criterion," *Journal of Information Security and Applications*, vol. 66, p. 103135, 2022.
[12] W. Zhang, Z. Bao, D. Lin, V. Rijmen, B. Yang, and I. Verbauwhede, "Rectangle: a bit-slice lightweight block cipher suitable for multiple platforms," *Cryptology ePrint Archive*, 2014.
[13] C. De Canniere, A. Biryukov, and B. Preneel, "An introduction to block cipher cryptanalysis," *Proceedings of the IEEE*, vol. 94, no. 2, pp. 346–356, 2006.
[14] J. Lim, D. Ng, and R. Ng, "Sok: Security evaluation of sbox-based block ciphers," *Cryptology ePrint Archive*, 2022.
[15] M. Stamp and R. M. Low, *Applied cryptanalysis: breaking ciphers in the real world*. John Wiley & Sons, 2007.
[16] C. Carlet, "Boolean functions for cryptography and coding theory," 2021.
[17] W. Zhang, Z. Bao, V. Rijmen, and M. Liu, "A new classification of 4-bit optimal s-boxes and its application to present, rectangle and spongent," in *Fast Software Encryption: 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers 22*, pp. 494–515, Springer, 2015.
[18] Y. Tong, S. Xu, J. Huang, B. Wang, and Z. Ren, "A new analysis of small s-boxes based on a new notion of algebraic immunity," *Journal of Information Security and Applications*, vol. 77, p. 103574, 2023.
[19] D. E. Standard *et al.*, "Data encryption standard," *Federal Information Processing Standards Publication*, vol. 112, p. 3, 1999.
[20] G. Orhanou, S. El Hajji, and Y. Bentaleb, "Snow 3g stream cipher operation and complexity study," *Contemporary Engineering Sciences-Hikari Ltd*, vol. 3, no. 3, pp. 97–111, 2010.
[21] M. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, "A new design of cryptosystem based on s-box and chaotic permutation," *Multimedia Tools and Applications*, vol. 79, pp. 19129–19150, 2020.
[22] K. Nyberg, "Differentially uniform mappings for cryptography," in *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 55–64, Springer, 1993.
[23] D. R. Stinson, *Cryptography: theory and practice*. Chapman and Hall/CRC, 2005.
[24] T. S. Developers, *SageMath, the Sage Mathematics Software System (Version 9.6)*, 2022. https://www.sagemath.org.
[25] L. Cheng, W. Zhang, and Z. Xiang, "A new cryptographic analysis of 4-bit s-boxes," in *Information Security and Cryptology: 11th International Conference, Inscrypt 2015, Beijing, China, November 1-3, 2015, Revised Selected Papers 11*, pp. 144–164, Springer, 2016.
[26] M. Durasevic, D. Jakobovic, L. Mariot, S. Mesnager, and S. Picek, "On the evolution of boomerang uniformity in cryptographic s-boxes," in *International Conference on the Applications of Evolutionary Computation (Part of EvoStar)*, pp. 237–252, Springer, 2023.
[27] G. Leander and A. Poschmann, "On the classification of 4 bit s-boxes," in *Arithmetic of Finite Fields: First International Workshop, WAIFI 2007, Madrid, Spain, June 21-22, 2007. Proceedings 1*, pp. 159–176, Springer, 2007.
[28] D. C. Ventura, L. M. R. Henríquez, and S. E. P. Hernández, "Requirements for feistel-based lightweight block cipher s-boxes to be resilient to boomerang attacks," in *2023 Mexican International Conference on Computer Science (ENC)*, pp. 1–8, 2023.

Estado Actual de los Algoritmos Post-Cuánticos

Kevin A. Delgado Vargas[1], Gina Gallegos-García[2]
Instituto Politécnico Nacional
Escuela Superior de Ingeniería Mecánica y Eléctrica. Unidad Culhuacan
Sección de Estudios de Posgrado e Investigación
Av. Santa Ana 1000, San Francisco Culhuacan, Culhuacan, 04430, Ciudad de México.
kdelgadov1200@alumno.ipn.mx[1], ggallegosg@ipn.mx[2]

***Resumen*—Desde los inicios de la criptografía, su objetivo siempre ha sido preservar diferentes servicios de seguridad de la información. Sin embargo, dado que el poder de cómputo ha avanzado a pasos agigantados, algunos de los algoritmos que actualmente preservan los servicios de confidencialidad, autenticación, integridad y no repudio, han sido rotos y como consecuencia, los sistemas de la industria que los utilizan, también. Con computadoras cada vez más potentes, como las cuánticas, la criptografía se ha visto amenazada cada vez más y más, es por ello que la comunidad científica ha hecho énfasis en algoritmos que sean capaces de resistir ataques provenientes de cualquier tipo de computadora, haciendo un llamado a una estandarización de nuevos algoritmos llamados algoritmos post-cuánticos.**

***Index Terms*—Algoritmos criptográficos, criptografía post-cuántica, estandarización de algoritmos, primitivas criptográficas, servicios de seguridad**

I. Introducción

A lo largo de los tiempos, la criptografía ha jugado un papel muy importante, debido a que desde sus inicios se ha enfocado en estudiar las técnicas matemáticas relacionadas a los aspectos de la seguridad de la información, tales como, confidencialidad, integridad de los datos, autenticación de entidad y no repudio [1].

Históricamente hablando, esta ciencia se divide en clásica, moderna, cuántica y post-cuántica.

La criptografía clásica tuvo sus inicios aproximadamente en el año 1900, antes de Cristo, con el primer registro de la escritura egipcia [2]. En aquel entonces se hacía uso de sustituciones y permutaciones para poder transformar la información ante terceras entidades no deseadas.

Con la criptografía moderna, alrededor de los años 70's, se introducen dos formas distintas de preservar los servicios de seguridad de la información, ya que en ella se utilizan algoritmos criptográficos de llave simétrica y de llave asimétrica [1].

A la par, en esa misma década, es que se tienen las primeras ideas relacionadas con la criptografía cuántica, las cuales basan su seguridad en los pricipios de la mecánica cuántica, como el principio de la incertidumbre o el principio de la superposición [5], con lo que este tipo de criptografía empezó a representar una amenaza inminente para la gran mayoria de los algoritmos que correspondientes a la criptografía moderna. Es decir, aquellos algoritmos que se creen seguros ante los ataques efectuados por computadoras clásicas. Debido a ello, es que en los años 90's es que surge la criptografía post-cuántica, que trae consigo algoritmos criptográficos que estan diseñados para resistir ataques efectuados por computadoras tanto clásicas como cuánticas.

Con base en lo anterior, en este trabajo se presenta una breve revisión del estado actual que guardan los algoritmos post-cuánticos, para tal fin el resto del artículo se organiza de la siguiente manera, en la Sección II, se presenta una definición de las primitivas criptográficas, y con base en la clasificación de los algoritmos criptográficos, se asocian los servicios de seguridad que pueden preservarse con ambos. La Sección III, especifica lo que es la criptografía post-cuántica, así como los tipos de algoritmos en los que ésta se clasifica. La Sección IV presenta la lista de organizaciones que se han enfocado en el trabajo de la estandarización de los mismos, enfocándose en el nivel de seguridad que ellos deben tener. En la Sección V se listan algunos de los retos que aún presenta el uso de algoritmos post-cuánticos. Por último, se muestran las conclusiones y se listan las referencias.

II. Primitivas y Clasificación de Algoritmos Criptográficos

Criptográficamente hablando, las primitivas criptográficas son herramientas utilizadas para preservar los servicios de seguridad antes mencionados. Estas pueden ser evaluadas con respecto a cinco criterios, siendo estos los que se enlistan a continuación:

1. Nivel de seguridad: Este normalmente es difícil de cuantificar. Sin embargo, el nivel de seguridad se da en términos del número de operaciones requeridas para derrotar un objetivo previsto.
2. Funcionalidad: Las primitivas deben combinarse para preservar un servicio de seguridad. La determinación de la mejor primitiva para preservar un servicio está determinada por la propiedad de la misma.
3. Métodos de operación: Las primitivas, dependiendo de la manera en la que se empleen y de las entradas que tengan, van a obtener características diferentes; por lo tanto, una misma primitiva puede presentar una funcionalidad diferente dependiendo de su modo de operación o su uso.
4. Desempeño: Este criterio hace referencia a la eficiencia de una primitiva en un modo particular de operación.
5. Facilidad de implementación: Implica la complejidad de implementar una primitiva en una instalación práctica,

ya sea un entorno de software o hardware [1].

De manera general estas herramientas abstractas se clasifican en: primitivas criptográficas sin llave, primitivas con llave, de hash y de números pseudoaleatorios. Esta clasificación está vinculada con los algoritmos criptográficos que permiten que dichas abstracciones materialicen los distintos servicios de seguridad de la información. De ahí, que con base en la cantidad de llaves que se utilizan, los algoritmos pueden clasificarse en algoritmos de llave simétrica y algoritmos de llave asimétrica. Los algoritmos criptográficos simétricos utilizan una sola llave para hacer/deshacer las transformaciones hechas a la información.
Estos, a su vez y considerando la forma en como manipulan la información, se dividen en algoritmos de bloque y algoritmos de flujo. Los primeros manipulan la información en bloques de longitud k, siendo k definido por el algoritmo en específico. Los de flujo, manipulan la información con correspondencias bit a bit sobre el flujo mismo. Por otro lado, los algoritmos de llave asimétrica utilizan un par de llaves para llevar a cabo las transformaciones a la información.
Ambos son utilizados en computadoras con arquitectura Von Neumann y Harvard y han ido evolucionando a tal grado que con el advenimiento de computadoras cada vez más potentes y con el aumento de su uso para procesar y transmitir información rápidamente, se presentan nuevas exigencias frente a los algoritmos criptográficos, surgiendo la necesidad de utilizar algoritmos capaces de resistir ataques de computadoras cuánticas. Lo anterior, aunado al rompimiento de algoritmos simétricos y asimétricos, ha hecho que la comunidad científica se enfoque en un reciente conjunto de algoritmos llamados, post-cuánticos.

III. Rompimiento de Algoritmos Modernos

En los años 90's los algoritmos criptográficos modernos empezaron a verse afectados por la computación cuántica, y que el matemático Peter Shor, desarrolló un algoritmo para encontrar factores de un número de una forma eficiente. Su implementación pudo llevarse a cabo de manera clásica o utilizando circuitos cuánticos [3]. Este algoritmo basa su potencia en determinar el periodo de una función, para que de esta manera se puedan encontrar factores primos para un entero. De ahí que un ordenador cuántico con un número suficiente de qubits que ejecuten el algoritmo de Shor, podría utilizarse para romper algoritmos modernos de llave asimétrica.
Por otro lado, en 1997, K. L. Grover, publicó el llamado Algoritmo de Grover [4], siendo desde aquel entonces, una amenaza para algunos de los algoritmos criptográficos modernos, ya que este reduce efectivamente a la mitad los niveles de seguridad. Esto, ya que para el caso del algoritmo simétrico AES-256, este se renderiza igual que AES-128 ejecutando el algoritmo de Grover en un ordenador cuántico suficientemente potente.
Por lo tanto, los algoritmos post-cuánticos no necesitan cambiar significativamente de la criptografía simétrica moderna, siguiendo obteniendo los niveles de seguridad actuales.

IV. Algoritmos Criptográficos Post-cuánticos

Dependiendo de la funcionalidad y del problema en el que basan su seguridad, los algoritmos post-cuánticos se clasifican en 4 tipos, algoritmos basados en código, algoritmos basados en Hash, basados en rejillas (Lattices) y algoritmos basados en polinomios cuadráticos multivariables.

IV-A. Algoritmos basados en Código

Son aquellos que usan, como elemento fundamental, un código de corrección de errores C. Este elemento fundamental puede consistir en añadir un error a una palabra de C o en calcular un síndrome respecto a una matriz de comprobación de paridad de C. Uno de los primeros algoritmos basados en código, es el algoritmo de McEliece [6], base de los algoritmos que actualmente están siendo diseñados.

IV-B. Algoritmos basados en Hash

La seguridad de los esquemas de firma digital que se usan en la práctica actual, a menudo se basan en la dificultad de factorizar enteros grandes y calcular logaritmos discretos. Las firmas digitales han llegado a ser un elemento clave para preservar autenticidad, integridad y no repudio de los datos. Los algoritmos de firma digital usados en la práctica hoy en día, no son inmunes a ataques efectuados por computadoras cuánticas, dado que su seguridad recae en la dificultad de factorizar enteros grandes y calcular logaritmos discretos. De ahí, que los algoritmos de firma basados en hash y que resisten ataques hechos por computadoras cuánticas, utilizan una función hash, al igual que las demás, pero con la diferencia de que su seguridad recae en la resistencia a colisiones de la propia función hash. De hecho, la existencia de funciones hash resistentes a colisiones se puede ver como un requisito mínimo para la existencia de un algoritmo de firma post-cuántico, esto dado que los algoritmos de firma mapean documentos de longitud arbitraria hacia firmas digitales de longitud fija, lo que muestra que el algoritmo de firma es en sí, una función hash.
Los primeros autores en presentar este tipo de construcciones fueron Lamport [7], siendo mejorados por Merkle [8] y Winternitz, donde la propuesta una sola via de Winternitz es una generalización de la propuesta de una sola vía de Merkle [9].

IV-C. Algoritmos basados en Rejillas (Lattices)

Las construcciones criptográficas basadas en rejillas son una gran promesa como parte de los algoritmos post-cuánticos. Muchos de ellos son bastante eficientes, y algunos otros compiten con las alternativas más conocidas, son simples para implementar y por supuesto, se creen seguros en contra de computadoras cuánticas. En términos de seguridad, las construcciones criptográficas basadas en rejillas, se dividen en dos tipos, el primer tipo incluye propuestas clásicas que son típicamente eficientes, pero carecen de pruebas de seguridad. El segundo tipo ofrece garantías de seguridad demostrable para los problemas de lattices del $peorcaso$. Es decir, que el rompimiento de la construcción criptográfica, inclusive con

probabilidad no-despreciable, es al menos tan difícil como resolver algunos problemas de las rejillas en el $peorcaso$. En otras palabras, romper la construcción criptográfica implica un algoritmo eficiente para resolver cualquier instancia de algún problema de rejilla en cuestión. La primera propuesta de algoritmo basado en rejillas fue hecho por Hoffstein, Pipher y Silverman en los años 90's, lo llamaron NTRU [10] y tiene la característica de trabajar con llaves más pequeñas que las que se tiene en el algoritmo McEliece [6].

IV-D. Algoritmos basada en Polinomios Cuadráticos Multivariables

También conocida como criptografía basada en polinomios multivariable, es el término general para definir aquellos algoritmos que trabajan con polinomios de multiples variables sobre un campo finito como su elemento público. De ahí que, por ejemplo, si los polinomios tienen grado dos, entonces se está hablando de polinomios cuadrados multivariables. Su seguridad descansa en la $dificultad - NP$ del problema para resolver ecuaciones no lineales sobre campos finitos. Esta familia, se considera como una de las familias más grandes de llave asimétrica que pudieran resistir poderosos ataques efectuados por computadoras cuánticas. Los algoritmos correspondientes a esta clasificación permiten un rápido cifrado y descifrado de datos así como una veloz generación y verificación de firmas. El primer registro de algoritmos multivariables fue el Imaí-Matsumoto en el año 1988 [11].

V. Estandarización de algoritmos post-cuánticos

Algunos cuerpos de estandarización han reconocido la urgencia de cambiar y utilizar algoritmos que sean seguros ante ataques hechos por computadoras cuánticas. Esto es muy importante dado que muchas aplicaciones criptográficas requieren que todas las entidades participantes utilicen el mismo algoritmo, de ahí que la estandarización de algoritmos es un pre-requisito para el amplio uso de los mismos.

De hecho, algunos estándares de-facto son tomados por distintos cuerpos de estandarización, pero los procesos formales de estandarización son ampliamente vistos como una forma de reducir riesgos.

El grupo de trabajo de ingeniería en internet, IETF por sus siglas en ingles [12], y su rama de investigación IRTF se encuentran como líderes terminando la estandarización de algoritmos de firma basados en hash. Algunas otras organizaciones que están interesados en la estandarización de la criptografía post-cuántica son la ETSI [13], con su grupo de trabajo llamado "quantum-safe". De igual forma, ISO [14] con SC27 WG2 y OASIS [15] con el estándar de KMIP. Por su parte el Instituto Nacional de Estándares y Tecnología (por sus siglas en ingles NIST) en el año 2017 empezó un proceso de solicitud, evaluación y estandarización de uno o más algoritmos de asimétricos, resistentes a ataques cuánticos. Este proceso será de múltiples rondas de evaluación y durará aproximadamente de 3 a 5 años [16]. Cabe destacar que en la primera ronda de evaluación se recibieron alrededor de 70 propuestas, las cuales tuvieron que cumplir con los requisitos mínimos de aceptabilidad, presentación y de evaluación para los algoritmos candidatos. De los candidatos recibidos en esta ronda de evaluación, al menos 5 fueron descartadas debido a las críticas realizadas por la comunidad científica.

V-A. Niveles de seguridad aplicables a los algoritmos post-cuánticos

En el año 2001 el NIST emitió el Estándar Federales de Procesamiento de la Información 140-2 (FIPS por sus siglas en Inglés) el cual se enfoca en detallar la acreditación de módulos criptográficos desde el punto de vista de componentes de software y desde el punto de vista de hardware [17]. Este estándar considera, entre otras cosas, los 4 niveles de seguridad a los que se deben ajustar todos los módulos criptográficos y son los niveles en los que basan su seguridad, aquellos algoritmos post-cuánticos que están siendo estandarizados, actualmente, por el NIST. Estos son descritos a continuación:
Nivel 1: El nivel más bajo de seguridad, no especifica un mecanismo de seguridad físico, pero si impone requisitos de seguridad básicos. Es utilizado para componentes de software y firmware de un módulo criptográfico.
Nivel 2: Este nivel de seguridad requiere, como mínimo, la autenticación basada en roles en la que un módulo criptográfico autentica la autorización de un operador basado en el cargo del usuario.
Nivel 3: En este nivel de seguridad, se añade una resistencia a la intrusión física. Así mismo incluye protección criptográfica eficaz y administración de llaves, además de la autenticación basada en identidad y separación física o lógica.
Nivel 4: El máximo nivel de seguridad incluye protección avanzada contra intrusos, además de que este puede funcionar en entornos que no estén protegidos físicamente.

V-B. Algoritmos post-cuánticos clasificados por el Instituto Nacional de Estándares y Tecnología

Las propuestas de algoritmos recibidas por el NIST se basan en la clasificación de los cuatro tipos que se mencionaron en la Sección III, siendo estos: algoritmos basados en códigos, algoritmos basados en hash, algoritmos basados en rejillas y basados en criptografía multivariable. Cabe destacar que varias de las propuestas recibidas se enfocan en preservar diferentes servicios, esto con base en sus respectivas primitivas criptográficas. Es decir, a la fecha se está trabajando en la estandarización de algoritmos post-cuánticos de llave publica para la primitiva de cifrado y firma, así como en algoritmos de intercambio de llaves. Ejemplo de ello, son los algoritmos post-cuánticos que basan su funcionalidad en rejillas y en polinomios multivariables, que tienen propuestas para cifrado y firma.

VI. Retos existentes dentro de los algoritmos post-cuanticos

De todas las propuestas antes mencionadas enviadas al NIST, se puede hacer una clasificación de los algoritmos dependiendo de su tipo de criptografía.

En términos generales una de las preocupaciones que se tiene con los algoritmos post-cuánticos, es el uso de ellos dentro de los sistemas de la industria, de ahí los restos y áreas de oportunidad se citan a continuación:

- Tamaño de llaves. En muchos de los casos, los algoritmos hacen uso de llaves muy grandes, esto genera que la velocidad de procesamiento se vea reducida significativamente.
- Firmas cortas. Si el tamaño de las llaves disminuye, entonces el tamaño de las firmas también lo hará, generando una velocidad de firmado más rápida.
- Velocidad en cifrado, firma y verificación. Existe una relación entre la velocidad y los tamaños de firmas y de llaves, puesto que mientras más grande sean estos, la velocidad disminuye.
- Flexibilidad y adaptación entre distintos algoritmos. El proceso de estandarización no especifica que los algoritmos deben trabajar solos, es decir, que no pueden trabajar en conjunto con algún otro algoritmo. Algunos de los algoritmos post-cuánticos son capaces de trabajar mano a mano con otros algoritmos, por lo cual generan mayor protección, esto les da una ventaja sobre los demás competidores.
- Utilizar como base algoritmos cuya resistencia este comprobada ante ataques cuánticos. Existen algunos algoritmos que se creen seguros ante ataques de computadoras cuánticas, pero la mayoría de los algoritmos recibidos por el NIST, no hacen uso de ellos por lo tanto su resistencia ante los ataques cuánticos no está comprobado.
- Eficiencia de memoria. La ventaja que tienen estos algoritmos es el poco espacio de memoria que requieren para funcionar, pero aún podrían utilizar menos espacio si se reducen los tamaños de firmas y llaves.
- Facilidad de implementación. Los algoritmos post-cuanticos deben poder ser implementados de una manera sencilla en cualquier tipo de sistema dentro de la industria que así lo requiera, entre los que se destacan sistemas embebidos con muy pocos bits o computadoras clásicas.

Conclusiones

La revisión y el análisis de las referencias consultadas dejaron ver que aún queda mucha tarea por hacer y por corregir, esto, dado que una de las mayores preocupaciones reside en la forma en cómo se comportarían los algoritmos criptográficos post-cuánticos dentro de la industria, muestra de ello es la notoria participación de la comunidad científica tanto para diseñar este tipo de algoritmos como para estandarizarlos, lo cual conlleva a afirmar que no es solo una organización ni un solo grupo científico, sino, son varios los grupos de trabajo que alrededor del mundo, se encuentran llevando a cabo estas tareas, muestra de ello se ve con el NIST.

Parámetros como longitud de llaves, velocidad de cómputo y eficiencia, aún siguen siendo revisados y estudiados con mayor detalle. Esto, con la finalidad de mejorar aún más el comportamiento que tendrían estos algoritmos de manera conjunta con la industria.

Posibles trabajos a futuro consistirían en analizar la viabilidad del uso de algoritmos post-cuánticos dentro de propuestas de solución que interactúen de manera directa con la industria. Lo anterior, en escenarios industriales que hagan uso de diferentes redes de sensores, sistemas embebidos, aplicaciones móviles, bibliotecas criptográficas y lenguajes de programación, por mencionar algunos.

Agradecimientos

Los autores agradecen al Instituto Politécnico Nacional por el apoyo otorgado para la realización de este trabajo, a través de los proyectos SIP 1917 y 20180505.

Referencias

[1] A. Menezes, P. van Oorsschot, y S. Vanstone, *Handbook of Applied Cryptography*, primera edición, CRC Press, 1996.
[2] Caballero, P. (2002), *Introducción a la Criptografía.* Ed. Ra-Ma. Madrid
[3] Shor, P., *Algorithms for quantum computation: Discrete logarithms and Factoring.*, Proceedings 35th Annual Symposium on Foundations of Computer Science (1994), 124-134.
[4] K.L. Grover, *Quantum mechanicshelpsin searchingfora needlein a haystack*, Phys. Rev. Lett.79 (1997), 325-328.
[5] Chen, Lily; Jordan, Yi-Kai Liu; Moody, Dustin; Peralta, Rene; Smith-Tone, Daniel (April 2016). *Report on Post-Quantum Cryptography*
[6] McEliece y R. J. *A public-key cryptosystem based on algebraic coding theory* 1978.
[7] Lamport, L., *Constructing digital signatures from a one way function.* Technical Report, 1979.
[8] Merkle, R.C., *"A certified digital signature." in Proccedings on Advances in Cryptology* - CRYPTO '89 Proceedings,Springer-Verlag New York, Inc., 1989.
[9] Anders Fog, Bunzel, (2015). *Hash Based Digital Signature Schemes*.
[10] Hoffstein J., Pipher J.y Silverman J., *NTRU – A ring based public key cryptosystem*, LNCS 1423, 1998.
[11] Tsutomu Matsumoto y Hideki Imai, *Public quadratic polynomial-tuples for efficient signature-verification and message-encryption*, Springer, Berlin, 1988.
[12] IETF, 2018. [Online]. Available: https://www.ietf.org/. [Accessed: 07- Sep- 2018].
[13] S. Dahmen-Lhuissier, *"Quantum-Safe Cryptography"*, ETSI, 2018. [Online]. Available: https://www.etsi.org/ [Accessed: 08- Sep- 2018].
[14] "ISO - International Organization for Standardization", Iso.org, 2018. [Online]. Available: https://www.iso.org/home.html. [Accessed: 07- Sep- 2018].
[15] OASIS — Advancing open standards for the information society, Oasis-open.org, 2018. [Online]. Available: https://www.oasis-open.org/. [Accessed: 07- Sep- 2018].
[16] "Post-Quantum Cryptography Standardization — NIST". [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.
[17] NIST, *FIPS PUB 140-2: Security Requirements for Cryptographic Modules*, 2001.

Ventajas y retos del uso de la criptografía post-cuántica al preservar el servicio de autenticación en dispositivos con recursos limitados

Alfonso F. De Abiega-L'Eglisse[1], Kevin A. Delgado-Vargas[2], Gina Gallegos-García[3], Mariko Nakano-Miyatake[4], Ponciano J. Escamilla-Ambrosio[5]
[1−5] Instituto Politécnico Nacional. [1,4] Escuela Superior de Ingeniería Mecánica y Eléctrica. Unidad Culhuacan. Sección de Estudios de Posgrado e Investigación. Av. Santa Ana 1000, San Francisco Culhuacan, Coyoacan, 04430, Ciudad de México. CDMX.
[2,3,5] Centro de Investigación en Computación, Laboratorio de Ciberseguridad. Av. Juan de Dios Bátiz S/N, Nueva Industrial Vallejo, 07738 Ciudad de México. CDMX.
alfonso.deabiega@gmail.com[1], kdelgadov1200@alumno.ipn.mx[2], ggallegosg@ipn.mx[3], mnakano@ipn.mx[4], pescamilla@cic.ipn.mx[5]

***Resumen*—El uso de las computadoras y de los sistemas de comunicación trajo consigo, desde los años 60's, una demanda por parte del sector privado de contar con medios para proteger la información que se transmitía digitalmente, de forma tal que se pudieran preservar diferentes servicios de seguridad antes, durante y después de su envío y transmisión desde una entidad emisora hasta una entidad receptora. A la fecha, dicha demanda no solo se tiene por parte del sector privado, sino es una necesidad que tiene la sociedad y la industria, al utilizar dispositivos con características diversas día a día para tal fin. Específicamente hablando del servicio de autenticación, la criptografía y la biometría han unido esfuerzos tanto para identificar a las entidades que se comunican dentro de un sistema, como para mantener auténtica la información que viaja entre ellas. Sin embargo, la unión de estas vertientes de investigación trae consigo ventajas y retos cuando se utilizan para diseñar propuestas de solución en dispositivos con recurso limitado. Con base en ello, en este trabajo se presenta un panorama breve de las ventajas y los retos que mantienen los dispositivos de recurso limitado que se utilizan por la biometría, al combinarla con la criptografía post-cuántica. Esto, dentro de escenarios en donde se requiera preservar el servicio de autenticación.**

***Index Terms*—Autenticación, criptografía post-cuántica, dispositivos de recurso limitado, sensores, sistemas empotrados.**

I. Introducción

Autenticación es un servicio relacionado con la identicación, que se aplica tanto a la entidad emisora y a la entidad receptora, como a la información que se transmite entre ellos, de tal forma que las dos entidades se identifican entre sí, del mismo modo que la información entregada a través de un canal de comunicación.

El servicio de autenticación se subdivide en dos clases principales: autenticación de entidad y autenticación de origen de datos, esta última proporciona implícitamente la integridad de los datos. Es decir, si se modifica un mensaje, la fuente podría haber cambiado.

Existen dos líneas de investigación que preservan el servicio de autenticación, la criptografía y la biometría. Cada una de ellas tiene tareas específicas y problemáticas que resuelven de manera independiente, incluso desde hace algunos años han unido esfuerzos para el diseño de propuestas de solución. Con base en ello, en este trabajo se hablará de las ventajas y retos que guarda cada una de ellas, cuando preservan el servicio de autenticación dentro de un escenario con dispositivos de recursos limitados.

II. Autenticación desde un punto de vista criptográfico

Las primitivas criptográficas pueden verse como herramientas abstractas que ayudan a preservar cuatro servicios de seguridad en la información: confidencialidad, integridad de los datos, autenticación y no repudio. Éstas se dividen en aquellas que no hacen uso de una llave criptográfica, aquellas que hacen uso de llave simétrica y aquellas que hacen uso de llave asimétrica. Las firmas digitales son las primitivas criptográficas de llave asimétrica más conocidas para preservar la integridad de los datos y la autenticación (de entidad y autenticación de origen de datos). Adicionalmente a éstas, también existen técnicas criptográficas que son diseñadas para permitir a una entidad (el verificador), asegurarse de que otra entidad (el demadante) es quién dice ser, de tal forma que es posible detectar la falsificación de identidad.

III. Evolución de la criptografía

Históricamente hablando, la criptografía puede clasificarse en: clásica, moderna, cuántica y postcuántica. Pero independientemente de esta clasificación, en la actualidad se define como una ciencia que ha jugado un papel muy importante al dedicar sus esfuerzos a preservar diferentes servicios de seguridad mediante el uso de secuencias algoritmicas definidas bajo un esquema.

Haciendo un breve recorrido por la historia de esta ciencia, se puede destacar que en los años 70's, en plena estandarización de los algoritmos pertenecientes a la criptografía moderna,

por parte del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) [1], es que se tienen las primeras ideas relacionadas con la criptografía cuántica. En los 80's es cuando se muestran las primeras publicaciones de nuevas ideas que basaban su seguridad en los pricipios de la mecánica cuántica, destacando el de la incertidumbre o el principio de la superposición. Dichos principios utilizan láseres para emitir información en un fotón, elemento constituyente de la luz, logrando conducir información a través de fibras ópticas. Lo anterior, para garantizar el servicio de confidencialidad de la información transmitida [2].

IV. La criptografía post-cuántica en dispositivos de recursos limitados

A la fecha, los algoritmos de Shor [3] y Grover [4], son capaces de comprometer algunos de los algoritmos utilizados desde la criptografía moderna hasta estos días. De ahí, que los esquemas criptográficos post-cuánticos surgen de la necesidad de proteger las diferentes propuestas de solución criptográficas, de ataques realizados por computadoras cuánticas a gran escala, ya que estas últimas son capaces de resolver los problemas matemáticos empleados por los esquemas criptográficos modernos de llave asimétrica. Es decir, la criptografía post-cuántica se define como aquella que tiene como objetivo construir esquemas de llave asimétrica que sean seguros inclusive en contra de computadoras cuánticas.

Es por ello que la comunidad científica ha puesto un especial énfasis en la criptografía post-cuántica, enfocando sus esfuerzos en el diseño de esquemas que se clasifican en: aquellos basados en reticulos, basados en ecuaciones de multiples variables, esquemas basados en isogeneas de curvas elípticas y en códigos. Todos ellos capaces de cumplir los requisitos del actual proceso de estandarización [1], prometiendo preservar los diferentes servicios de seguridad de la información, ante ataques efectuados inclusive desde computadoras cuánticas.

El reto al que se enfrentan estos nuevos esquemas, al intentar sustituir los actuales esquemas modernos por los futuros esquemas estándar radica en el desconocimiento del comportamiento y desempeño de ellos, en los diferentes escenarios en donde se tienen entidades y dispositivos con características diversas, incluso con recursos limitados.

V. Clasificación de los dispositivos de recursos limitados

Los dispositivos de recursos limitados, se definen como elementos que combinan hardware y software para realizar tareas especificas con limitaciones de memoria (entre 128Kb y 2Mb aprox), poca potencia computacional (procesadores de 16 a 32 bits), ocasionalmente con pantallas de 97x54 pixeles) y que generalmente se alimentan de baterías [5]. Dadas sus características mínimas, este tipo de dispositivos por lo regular se utilizan en maquinas industriales, automóviles, cámaras, aplicaciones de hogar y equipo médico, por mencionar algunos. Éstos, se pueden ordenar por capacidad, que van desde aquellos que solo fueron diseñados para cumplir una tarea muy específica, como la medición de algún dato, hasta aquellos que tienen una interfaz de usuario.

Los dispositivos de recursos limitados se pueden clasificar en dos tipos: el primer tipo correponde a aquellos de entrada o lectura y el segundo corresponde a aquellos dispositivos de procesamiento.

V-A. Dispositivos de lectura

Los del primer tipo son aquellos que a partir de una señal analógica o mecánica, entregan una señal digital. Ejemplos de ellos son los sensores corporales o los sensores biométricos. De hecho, uno de los escenarios de aplicación en donde es posible observar este tipo de dispositivos es en los escenarios médicos, con las conocidas redes de sensores, puesto que permiten monitorizar el estatus de los pacientes a través de las Redes Inalámbricas de Área Corporal (WBAN, por su acrónimo en inglés) [6], [7]. Estas redes involucran distintos sensores que están interconectados entre sí, y colocados en el cuerpo humano. La Figura 1 muestra la representación gráfica de una WBAN.

El otro ejemplo antes citado, corresponde a los sensores

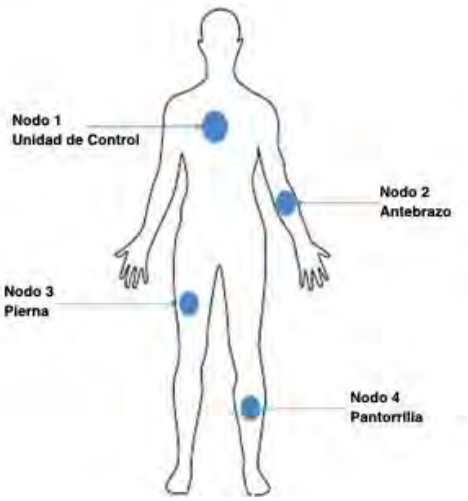


Figura 1. Distribución de sensores de lectura dentro de una Red Inalámbrica de Área Corporal

biométricos, definidos como aquellos dispositivos que transforman los rasgos biológicos, como el rostro, el iris o las huellas digitales; son escaneadas por medio de estos sensores y después de convertirlas en imagenes usando un convertidor analógico - digital de un individuo en señales eléctricas. Esta información digital de los datos biométricos son almacenados en memoria y utilizados para la verificación o autenticación de la identidad de una persona, conviertiéndose cada vez, en dispositivos importantes, útiles, efectivos, precisos y brindan seguridad. La Figura 2, muestra algunos de estos dispositivos biométricos. El escenario más reciente en donde se puede observar el uso de ellos es en la mayoría de los teléfonos inteligentes modernos, ya que incluyen al menos un sensor de huella digital para autenticar al usuario, mientras que los teléfonos

de gama alta proporcionan sensores biométricos adicionales como escáneres de iris y tecnología de reconocimineto facial.

Figura 2. Dispositivos de lectura de rasgos biológicos. Fuente: https://www.digitalavmagazine.com/2013/09/23/los-terminales-de-control-de-acceso-virdi-se-introducen-en-espana-de-la-mano-de-sti-card/

V-B. Dispositivos de procesamiento

El segundo tipo de dispositivos, son capaces de manejar todos los datos recibidos de los dispositivos de lectura o de otros de procesamiento.
Este tipo de dispositivos son diseñados para realizar una o algunas pocas funciones dedicadas, las cuales se obtienen a través de la programación, en lenguaje ensamblador, del microcontrolador o microprocesador incorporado sobre el mismo, o también, utilizando compiladores específicos o también se utilizan lenguajes como C o C++ [8]. En algunos casos, cuando el tiempo de respuesta no es un factor crítico, también, pueden usarse lenguajes Orientados a Objetos como JAVA.
Ejemplos de este tipo de dispositivos son mejor conocidos como sistemas embebidos o empotrados, como Arduino, Raspberry Pi, y BeagleBone, entre otros. Ellos son utilizados para cubrir necesidades específicas y la mayoría de sus componentes se encuentran incluidos en la placa base, utilizando un procesador relativamente pequeño y una memoria pequeña, como los que se observan en la Figura 3.

Figura 3. Dispositivos empotrados encargados del procesamiento de datos. Fuente: http://lasetecno.blogspot.com/p/que-es-un-sistema-embebido.html

VI. Identificación de ventajas y retos del uso de la criptografía post-cuántica en dispositivos con recursos limitados

Por lo regular, las propuestas de solución diseñadas para preservar un servicio de seguridad, como el servicio de autenticación, hacen uso de una combinación de dispositivos de lectura y procesamiento, quedando en una mezcla de dispositivos con características diversas y limitadas.
Específicamente hablando del servicio de autenticación, en los escenarios actuales, donde los dispositivos son cada vez más pequeños llegando a la restricción de tener recursos limitados, es que toma fuerza la importancia de que las entidades, que dicen estarse comunicando entre sí, son quienes dicen ser.
De hecho, los dispositivos de entrada tienen la ventaja de que pueden cumplir, de la manera mas óptima, con la función para la que fueron diseñados. Sin embargo, una de sus mayores desventajas es que estos dispositivos están "cerrados" por el fabricante, es decir que no se pueden reprogramar. Adicionalmente a esto, su calibración no es exacta, lo cual genera un margen de error. Uno de los retos asociados a este tipo de dispositivos, al momento de preservar el servicio de autenticación, es el diseñar el propio dispositivo de hardware criptográfico, creado a partir de la identificación de los requisitos que debe cumplir el dispositivo creado para la tarea que esté destinado a desarrollar.
Algunas de las carencias que se encuentran en los dispositivos de lectura, se compensan con los dispositivos de procesamiento, ya que estos se pueden programar y es posible almacenar y/o manejar los datos provenientes de los dispositivos de lectura. Es decir, éstos pueden tener tantos módulos de lectura como sean necesarios, así como una amplia gama de aplicaciones y propuestas de solución que de manera conjunta resuelvan problemas específicos.
Las diferentes propuestas de solución, enfocadas en preservar el servicio de autenticación, llegan a ser demasiado elaboradas, lo cual se ha llegado a solucionar haciendo uso de la criptografía de peso ligero, la cual demanda mínimamente el recurso del dispositivo. Un ejemplo de ello se puede observar dentro de las WBAN, ya que en este tipo de redes existen propuestas de solución que utilizan esquemas criptográficos de llave asimétrica para proveer el servicio de autenticación, con la característica de ser de peso ligero. Algunos otros hacen uso de algoritmos de curva elíptica, con la desventaja de que las soluciones que involucran el uso de la criptografía de curva elíptica consume aún más recursos, quedando un gran reto referente a la forma en cómo se comportarían los esquemas post-cuánticos dentro del escenario de las redes de sensores corporales.
Aunado a ello, otro reto existente reside en balancear la seguridad vs el desempeño y decidir qué vertiente de la criptografía post-cuántica debería considerarse para diseñar una propuesta de solución ecaminada a preservar el servicio de autenticación, ya que cada vertiente podría tener un comportamiento, velocidad de respuesta y uso de recurso diferente, cuando sea ejecutado en un dispositivo con las mis-

mas características. Esto, considerando que en los esquemas post-cuánticos, las claves son de una longitud considerable, generando que el nivel de seguridad que proporciona sea alto perdiendo velocidad de respuesta [9].
Además, hablando específicamente de la primitiva de firma y con base en la longitud de sus repectivas llaves, es evidente el tamaño de la firma digital que será obtenida. Ante esto, se deja ver como reto, el analizar si es posible que los algoritmos post-cuánticos, encargados de preservar el servicio de autenticación, pueden proveer el mismo nivel de seguridad que ofrecen los esquemas modernos Lo anterior, considerando el éxito que han tenido los esquemas criptográficos de peso ligero dentro de sensores de procesamiento con recursos limitados.

VII. Conclusiones

La importancia que tienen los diferentes servicios de seguridad radica en el escenario de aplicación en donde se preserva cada uno de ellos. Específicamente hablando del servicio de autenticación, el cual se utiliza en la mayoría de las tareas ejecutadas tanto en la industria como en la sociedad de manera cotidiana, poco a poco ha tomado mayor importancia. Esto, ya que las soluciones criptográficas que basan su seguridad en la dificultad de resolver problemas que se cree son difíciles, con la llegada de las computadoras cuánticas, serán vulneradas con mayor facilidad.
En la actualidad, aun cuando IBM y Google ya han anunciado que poseen computadoras cuánticas, no se tiene una fecha segura que indique cuándo, las computadoras cuánticas se usarán como computadoras personales o portátiles. Sin embargo, no se debe esperar su llegada para dar inicio a la identificación de las ventajas y los retos que traerá consigo dentro de escenarios de aplicación en donde interactúen dispositivos con características diversas.
Los dispositivos con recursos limitados son cada vez más comunes dentro de la sociedad y la industria en dónde dependiendo de las características del escenario, siempre deberá considerarse un balance entre el nivel de seguridad que se quiera obtener y la velocidad de respuesta que se tiene, de ahí que será importante contar con los diferentes estudios y comparativas que marquen la pauta de una dirección a seguir en términos de dicho balance.
Desde un punto de vista criptográfico cabe destacar que la criptografía post-cuántica representa una nueva etapa de la criptografía, la cual ha avanzado de la mano de los dispositivos en donde es utilizada. Ante esto, diferentes estudios indican que los esquemas post-cuánticos presentan velocidad de respuesta mayor al que presentan los esquemas modernos, dejando abierto el camino para conseguir que seran capaces de igualar o reducir los tiempos de procesamientos que muestran dentro de arquitecturas físicas diversas.
La combinación de la criptografía post-cuántica y la biometría parecen ser un buen aliado para la seguridad de los diferentes escenarios en la industria y en la sociedad. Desde el punto de vista biométrico, el diseño de dipositivos de lectura cada vez más pequeños, parecen ser necesitados cada día más y más, lo cual da pie a explorar sobre el diseño de dispositivos de lectura con capacidad propia de procesamiento, sin la necesidad de requerir de un dispositivo adicional.

Agradecimientos

Los autores agradecen al Instituto Politécnico Nacional por el apoyo otorgado para la realización de este trabajo, a través de los proyectos SIP 1917, SIP-20190264, SIP-20194938 y SIP-20196694.

Referencias

[1] National Institute of Standards and Technology. (2018). Retrieved from https://www.nist.gov/
[2] L. Chen, Y. L. Jordan, D. Moody, R. Peralta y D. Smith-Tone.*Report on Post-Quantum Cryptography* (2016).
[3] P. Shor, *Algorithms for quantum computation: Discrete logarithms and Factoring.*, Proceedings 35th Annual Symposium on Foundations of Computer Science (1994), 124-134.
[4] K.L. Grover, *Quantum mechanicshelpsin searchingfora needlein a haystack*, Phys. Rev. Lett.79 (1997), 325-328.
[5] T. Agarwal. *A Brief About Embedded System their Classifications and Applications.* 15-11-16, de Edgefx Technologies Pvt Ltd. (2015), Sitio web: https://www.efxkits.us/classification-of-embedded-systems/
[6] B. Latre, B. Braem, I. Moerman, C. Blondia, and P. Demeester, *A survey on wireless body area networks.* Wireless Networks, (2011), 17(1):1-18.
[7] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia,I. Moerman, S. Saleem, Z. Rahman, and K. S. Kwak, *Acomprehensive survey of wireless body area networks.* Journal of Medical Systems, (2012), 36(3):1065-1094.
[8] Salas Arriarán, Sergio. *Todo sobre sistemas embebidos*, SAXO, (2017).
[9] Delgado Vargas, Kevin Andrae. De Abiega L'Eglisse, Alfonso Francisco. Gallegos-Garcia, Gina y Cabarcas, Daniel. *Un acercamiento a la línea del tiempo de los algoritmos criptográficos*. Revista Digital Universitaria (RDU). (2019). Vol. 20, Núm. 5 Septiembre-Octubre. DOI:http://doi.org/10.22201/codeic.16076079e.2019.v20n5.a7

Una aproximación sistemática a los problemas de ciberseguridad en las redes VANET

Arizaga-Silva, Juan A
Ingeniería en Sistemas Automotrices
Universidad Politécnica de Puebla
Juan C. Bonilla, Puebla
juan.arizaga@uppuebla.edu.mx

Alonso-Pérez, *Marco A*
Ingeniería en Sistemas Automotrices
Universidad Politécnica de Puebla
marco.alonso@uppuebla.edu.mx

Etcheverry, Gibran
Departamento de Computación, Electrónica y Mecatrónica
Universidad de las Américas Puebla
gibran.etcheverry@udlap.mx

López-Bárcenas, Mónica
Ingeniería en Sistemas Automotrices
Universidad Politécnica de Puebla
monica.lopez@uppuebla.edu.mx

Martín-Ortíz, Manuel
Laboratorio Nacional de Supercomputo
B.Universidad Autónoma de Puebla
manuel.martin@correo.buap.mx

***Abstract*—Intelligent transport systems (ITS), which will allow efficient and controlled management of vehicular traffic and urban mobility in general within the so-called "smart cities", are fundamentally based on the development of new communication technologies.**

The VANET networks (Vehicular Ad-hoc Network) are a type of Ad-Hoc networks or wireless distributed mobile networks that will increase safety for users and vehicles in various automotive environments (urban and road) because of the new services offered to drivers and pedestrians. As a result of the communications augmentation, many types of attacks can occur in this kind of network, where every constituent element will need a different cybersecurity approach.

This article presents the high-value elements within VANET networks and the cybersecurity threats which they could be exposed to.

Keywords— cybersecurity, VANET, threats, asset, automotive security

I. INTRODUCCIÓN

Los sistemas inteligentes de transporte (ITS), que permitirán una gestión eficiente y controlada del tráfico de vehículos y la movilidad urbana en general, dentro de las llamadas ciudades "inteligentes" se basan fundamentalmente en el desarrollo de nuevas tecnologías de comunicación.

Las redes VANET (*Vehicular Ad-hoc Network*) son un tipo especial de redes móviles (MANET) con una estructura de red *Ad-Hoc* o una red móvil inalámbrica distribuida que se ha desarrollado para aumentar la seguridad de los usuarios y vehículos en diversos entornos automotrices, así como también brindar nuevos servicios a los conductores. y peatones.

Hay muchos tipos de ataques que pueden ocurrir en una red VANET (amenazas a la confidencialidad integridad y autenticidad de la información, robo de identidad), cada elemento dentro de la red necesita un enfoque de ciberseguridad diferente según su naturaleza. Este artículo, en su primera parte, muestra los antecedentes inmediatos de las redes VANET, para después, desde el punto de vista de ciberseguridad establecer los elementos de alto valor tanto tangibles como intangibles, los activos (*assets*) que hacen de las redes VANET el blanco de ataques cibernéticos; por último se exponen los diferentes tipos de amenazas a los que pueden estar expuestos cada uno de los diferentes activos en la red.

II. ANTECEDENTES

A) Redes VANET

En los últimos años, los automóviles han dejado de ser considerados un medio de transporte para convertirse en centros de datos móviles con la intención de incrementar la seguridad de los pasajeros y prevenir accidentes [1] ; para esto se han diseñado una gran variedad de aplicaciones móviles lo que ha creado un nuevo mercado, ante la necesidad de transferir la información de los autos o los ocupantes a través de Internet u otro tipo de red. La nueva generación de automóviles será capaz de realizar conexiones con su entorno, a través de lo que se ha dado a conocer como redes vehiculares, estas conexiones son diversas en aplicaciones y de diferente naturaleza: entre vehículos (V2V), con la infraestructura (V2I), con los peatones (V2P), entre otras; todas ellas agrupadas con el nombre de VANET's. (*Vehicular Ad-Hoc Networks*)[2].

Las redes VANET son un tipo de redes *Ad-Hoc* o de redes móviles distribuidas de naturaleza inalámbrica, formadas por dos tipos de nodos: estáticos y móviles. Los nodos estáticos, son elementos fijos emplazados a lo largo de las carreteras llamados RSU (*Road-Side Unit*), cuya función es la de enviar, recibir y retransmitir paquetes para aumentar el rango de cobertura de la red pudiendo también ofrecer acceso a Internet. Los nodos móviles son los vehículos equipados con un dispositivo electrónico llamado OBU (*On Board Unit*) para poder comunicarse con otros vehículos o con las RSU. Estos tipos de nodos tienen la capacidad de enviar, recibir y retransmitir mensajes entre ellos[3].

B) Tipos de conexión en las Redes VANET

Se han definido diferentes tipos de conexiones o escenarios de comunicación en las redes vehiculares: la comunicación intervehicular o vehículo a vehículo (V2V), en la que los automóviles intercambian mensajes directamente, la comunicación vehículo a infraestructura (V2I), la comunicación vehículo a RSU (V2R) y la comunicación vehículo a Peatón (V2P) [4].

Vehículo a Vehículo (V2V: *Vehicle to Vehicle*): Este tipo de comunicación se refiere a la comunicación directa o basada en multisaltos entre vehículos en una red VANET. Esto significa que los vehículos funcionan como receptor, emisor y ruteador de información a través de la red.

Vehículo a Infraestructura (V2I: *Vehicle to Infrastructure*): El escenario de comunicación V2I hace referencia a la conexión existente entre los vehículos y la infraestructura (semáforos, luminarias, avisos, casetas de peaje) a lo largo de la carretera.

Vehículo a Peatón (V2P: *Vehicle to Pedestrian*): V2P hace referencia a la comunicación entre los nodos de una red VANET y los peatones que circulan en un ambiente urbano.

Directo en el Vehículo (DIV: *Direct in Vehicle*): la comunicación DIV es poco referenciada por la literatura y se da cuando dos o más unidades de aplicación (AU) en el mismo vehículo intercambian información entre ellas; un ejemplo de esto es un dispositivo dentro del automóvil compartiendo acceso a Internet a otros dispositivos.

Vehículo a la red eléctrica (V2G:*Vehicle to Grid*) es un sistema en el que los vehículos eléctricos se comunican con la red eléctrica para devolver electricidad a la red o acelerar la velocidad de carga del vehículo. Será un elemento en algunos modelos de autos que se conectan a la red y se utiliza como un modulador de red eléctrica para ajustar dinámicamente la demanda de energía.

Vehículo a Hogar (V2H: *Vehicle to Home*): escenario propuesto por la ITU (*International Telecommunication Union*) para la convergencia de Redes de Nueva Generación con redes VANET. Hace referencia a la comunicación entre un nodo de una red vehicular con un nodo de una red fija en el hogar a través de una infraestructura de red de próxima generación (*Next Generation Network*) NGN [5].

Todos los tipos anteriores son agrupados según la literatura en el tipo genérico (V2X) *Vehicle to everything*.

III. Ciberseguridad en Redes VANET

Las redes VANETs son redes auto-organizadas diseñadas para la comunicación entre vehículos. En una VANET, cada vehículo se define como un nodo de la red Mediante la OBU los vehículos son capaces de comunicarse de forma inalámbrica entre sí, así como con las unidades de la carretera RSU. Los automóviles cuentan además con una unidad de aplicación llamada AU (*Application Unit*), las AU hacen referencia a los dispositivos que muestran información al usuario. Generalmente se les da esta denominación a dispositivos como computadores portátiles, smartphones o pantallas

Se espera que las redes VANET soporten una amplia gama de aplicaciones prometedoras tales como servicios basados en la ubicación. Sin embargo, la naturaleza de la difusión del medio inalámbrico permitiría a un agente adverso espiar las comunicaciones que contengan los identificadores de nodo, y estimar las ubicaciones de los nodos de comunicación con suficiente precisión para rastrear los nodos [5-7].

La implementación de la seguridad en las redes VANET tiene desafíos únicos. El caso es más complicado debido a los diferentes requisitos de las distintas aplicaciones. La seguridad para la difusión segura de la información se requiere un enfoque diferente al requerido para aplicaciones de gestión del tráfico debido a que existen diferentes tipos de ataques que pueden ocurrir dentro de una red VANET.

La clasificación de los tipos de ataques dentro de la literatura especializada depende en gran medida del grupo de investigación por lo que en este artículo se mostrará una aproximación a los problemas de ciberseguridad basada en los activos (assets) presentes dentro de una red VANET

Ejemplos de la diversidad de clasificaciones se presentan a continuación: Los investigadores Du y Zhu proponen en su trabajo [8] un modelo de árbol de ataque donde asignan a cada nodo del árbol una probabilidad de sufrir un ataque por parte de un agente externo. La probabilidad en cada nodo depende de tres atributos: costo de ataque, dificultad técnica y dificultad de descubrimiento.

Kaur et al [9] presentan cinco diferentes categorías de ataques, aunque no muestran evidencia de por qué realiza esta división, antes bien cita trabajos anteriores [6,7,10]. Por otro lado, Tyagi y Dembla proponen solo dos clasificaciones de ataque, internos y externos, sin imponer un criterio explícito de dicha división[3].

Al igual que con otros sistemas, los desafíos de seguridad de los vehículos autónomos y las redes vehiculares se pueden clasificar en términos generales en ataques a la confidencialidad, integridad, privacidad y disponibilidad como lo mencionan Gerla y Reiher [11]; los otros sistemas a los que se refieren estos autores corresponden a sistemas ciberfísicos que soportan infraestructura crítica y sistemas de información gubernamental y empresarial donde es necesario asegurar los activos (valores tangibles e intangibles) de las organizaciones.

Esta diversidad de clasificaciones si bien ayuda a catalogar los distintos trabajos realizados desde diferentes ópticas no responde a las necesidades de la industria automotriz la cual ha desarrollado su propio marco de referencia[20].

Los activos son los objetivos potenciales de un atacante que son críticos para el correcto funcionamiento del sistema y los intereses de los grupos interesados , es decir, los elementos que deben protegerse. En otras palabras, la identificación de los activos debe estar alineada con los objetivos comerciales y los marcos regulatorios obligatorios.

Desde el punto de vista de ciberseguridad, los siguientes elementos son considerados activos dentro de las redes VANET [12]:

1) Usuario de la red VANET: Al ser una red concebida para incrementar la seguridad física de los automovilistas, éstos constituyen, junto con su información privada, el activo más importante de la red.

2) Intercambio de información: Al igual que otras redes, los usuarios de las redes Vehiculares también exigen seguridad en términos de integridad de datos, confidencialidad y disponibilidad (CIA por sus siglas en inglés: *confidentiality, integrity and availability*).

3) Vehículos: Dentro de las redes VANET los automóviles representan un activo importante por las tareas que realizan al interior de la red. Un vehículo en la actualidad más que un medio de transporte se ha convertido en un centro de datos móvil. Al interior del vehículo se encuentran los sensores que colectan la información que después será transmitida a través de la red utilizando la OBU hacia los nodos adyacentes al vehículo.

El automóvil puede también, como se ha mencionado anteriormente, transmitir, recibir y rutear paquetes de información hacia los demás elementos de la red.

4) Unidades en carretera (RSU) Este elemento sirve como puente entre el entorno de infraestructura y el entorno ad-hoc. En estos nodos se instalarán los sensores necesarios, las unidades de procesamiento y el sistema de comunicación para recibir información de otros nodos. Debido a su naturaleza estática es un activo con una alta probabilidad de ser atacado. Si la RSU se ve comprometida, los datos almacenados en el interior se ven comprometidos y no se puede garantizar la comunicación segura con la infraestructura.

5) Protocolos de comunicación de red: Las comunicaciones en una red VANET son por su naturaleza principalmente inalámbricas, el estándar de facto para comunicaciones vehiculares son las Comunicaciones Dedicadas de Corto Alcance (DSRC).

El DSRC se basa en la tecnología IEEE 802.11 y ha sido titulado bajo el nombre de IEEE 802.11p. Estas comunicaciones pueden incluir información de tráfico, información de accidentes, condiciones de la carretera, mensajes de seguridad entre vehículos,cobro de peaje, manejo a través del pago, etc. Otros dos estándares, el ASTM E2213-03 y el IEEE 1609.x conforman el estándar conocido como Acceso inalámbrico en entornos vehiculares (WAVE)[2].

Por otro lado las comunicaciones intravehiculares para conexión de los sensores y las ECU's del auto con la OBU se realizan a través del Bus CAN y Ethernet Automotriz.

6) Entidad central: La entidad central es otro nodo estático en la arquitectura VANET que incluye los servidores de aplicaciones que proporcionan diversas aplicaciones, como aplicaciones para evitar colisiones, actualizaciones del clima y el tráfico, etc.

La entidad central se encuentra en el dominio de la infraestructura y desempeña un papel vital durante la comunicación V2I donde los mensajes son recibidos primero por el servidor de aplicaciones. Autentica el mensaje recibido y lo reenvía a otros vehículos a través de una ubicación geográfica amplia[12].

7) Terceros en la red: Los terceros en la red representan a los distintos tipos de autoridades (policía y tránsito), los cuales se encuentran en la parte de la red VANET que representa la Infraestructura. También se incluye a los fabricantes de los automóviles, los cuales a través de canales dedicados de comunicación pueden tener acceso a la red intravehicular, al OBU o la Unidad de aplicación.

Es necesario asegurarse que los terceros sean confiables a través de algún elemento de seguridad, cuando esto sucede, son conocidos como TTP (*trusted third parties*)

IV. Amenazas de seguridad.

Esta sección presenta diversas amenazas potenciales para los activos de las redes VANET

A) Riesgos sobre los usuarios

A nivel de Usuario de la red las principales amenazas están relacionadas con la confidencialidad de la información personal del usuario así como su localización geográfica y otra información sensible.

Por ejemplo, se prevé que los servicios ofrecidos en VANET incluyan conexión a Internet y aplicaciones peer to peer para compartir archivos entre usuarios de la red. Un agente adversario podría generar aplicaciones maliciosas que sustraigan mayor información de los usuarios o que incluso pueda existir robo de identidad.

Otra amenaza hacia los usuarios de las redes VANET, como cualquier otra red es aquella basada en ingeniería social (*Physhing* o *spoofing*).

B) Amenazas a nivel de información

Siempre existen amenazas a la información donde el principal interés del atacante es comprometer su confidencialidad, integridad y autenticidad (CIA). Las amenazas a la información pueden explotarse siguiendo diferentes aspectos de seguridad

Al interior del vehículo, se ha comprobado que existen diversos ataques a las comunicaciones internas del vehículo, específicamente en el Bus de comunicaciones CAN [19], lo que podría dar lugar al envío de información errónea por parte de un usuario a los demás nodos de red, sobre todo en comunicaciones V2V y V2I, sobre diferentes aspectos relacionados a la velocidad y posición de un nodo móvil de la red[14].

C) Amenazas a la confidencialidad, integridad y disponibilidad de la información.

Un nodo de red puede actuar de manera maliciosa de diferentes formas, cada de una de ellas puede clasificarse como un intento de manipulación de la información.

Por ejemplo, cada nodo dentro de la red puede servir de puente como ruteador de la información entre dos nodos, cuando por algún motivo no conocido un nodo decide no retransmitir los paquetes de datos ante una solicitud es entonces cuando la disponibilidad de la información se ve alterada y la seguridad de los usuarios, automovilistas y peatones se ve en riesgo.

Por otro lado la confidencialidad de los paquetes de datos puede verse vulnerada al existir algún canal inalámbrico inseguro con un cifrado que resulte ineficiente[15].

De igual forma la integridad de la información se ve comprometida cuando un atacante externo puede alterar, modificar e incluso borrar paquetes de datos transmitidos entre varios elementos de la red.

Existen diversos vectores de potenciales amenazas a la información [10,12]:

- Escuchas de datos confidenciales.
- Ataque de interferencia (*Jamming*).
- Ataques de suplantación
- Ataques de hombre en el medio *Man in the middle*(MITM).
- Ataques de suplantación de identidad (*Spoofing*).

D) Amenazas a la infraestructura (RSU y Entidad central)

La infraestructura, siendo la entidad estática en VANET, es una de las ubicaciones favoritas para que un atacante lance diferentes ataques de red del tipo Denegación de Servicio (DoS) y del tipo Hombre en el medio (MITM), para generar alteración de mensajes en el canal y ataques de suplantación [17].

La forma de los ataques pueden ser del tipo[12,14,19]:

- Envío de mensajes comprometidos.
- Caída de mensajes.
- Fuga de datos en el canal cableado del *back-end.*
- Inundación de red con mensajes.
- Alteraciones de mensajes en ruta a otros vehículos a través de RSU y entidad central
- Ataques relacionados con la calidad (QoS) del mensaje

Como puede observarse en algunos dominios los tipos de ataques se superponen. Esto se debe a la naturaleza heterogénea de las redes VANET las cuales cubren diferentes tipos de protocolos, topologías y medios de transmisión

V. Conclusiones

En las últimas dos década, se han emprendido muchos proyectos VANET al rededor del mundo y se han desarrollado varios estándares VANET para mejorar las comunicaciones entre vehículos (V2V) y vehículo a otros (V2X). La existencia de redes VANET abre el camino para una amplia gama de aplicaciones y ha abierto la puerta a diversos riesgos de ciberseguridad.

En este trabajo se ha presentado una revisión de los elementos de alto valor dentro de las redes VANET; también se revisaron algunas de las principales amenazas de ciberseguridad en las que los investigadores han centrado su atención en los últimos años. Así como los diversos tipos de ataques que pueden surgir derivados de estas amenazas.

Referencias

[1] Jindal, V. and Bedi, P. “Vehicular ad-hoc networks: Introduction , standards , routing protocols and challenges” (2016).

[2] Arizaga-Silva J. Alonso-Perez M. Álvarez-González R., “Redes VANET Vehicular Ad-Hoc Networks, la conectividad de los autos. Primera parte.” 2018 Revista Visión Politécnica. Universidad Politécnica de Puebla.

[3] Tyagi and D. Dembla, “Advanced Secured Routing Algorithm of Vehicular Ad-Hoc Network,” Wireless Personal Communications, vol. 102, no. 1, pp. 41–60, May 2018.

[4] Al-Sakib Khan Pathan “Mobile ad hoc network and vehicular ad-hoc network security,” Security of self-organizing networks, CR Press. 2019

[5] Al-Sultan, S., Al-Doori, M. M., Al-Bayatti, A. H. & Zedan, H. A comprehensive survey on vehicular ad hoc network. J. Netw. Comput. Appl. 37, 380–392 (2014).

[6] Hoa La and A. Cavalli, "Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey", International Journal on AdHoc Networking Systems, vol. 4, no. 2, pp. 1-20, 2014.

[7] J. Isaac, S. Zeadally and J. Cámara, "Security attacks and solutions for vehicular ad-hoc networks", IET Communications, vol. 4, no. 7, p. 894, 2010.

[8] Du and H. Zhu, “Security Assessment in Vehicular Networks,” SpringerBriefs in Computer Science, 2013.

[9] R. Kaur, T. P. Singh, and V. Khajuria, “Security Issues in Vehicular Ad-Hoc Network(VANET),” 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), May 2018.

[10] "VANET, its Characteristics, Attacks and Routing Techniques: A Survey", International Journal of Science and Research (IJSR), vol. 5,no. 5, pp. 1595-1599, 2016.

[11] M. Gerla and P. Reiher, “Securing the Future Autonomous Vehicle: A Cyber-Physical Systems Approach,” Securing Cyber-Physical Systems, pp. 197–220, Sep. 2015.

[12] Ahmad, F., Adnane, A. and N. L. Franqueira, V. (2016) “A Systematic Approach for Cyber Security in Vehicular Networks”. Journal of Computer and Communications, 4, 38-62.

[13] Nadeem Majeed, M. e. a. Vehicular ad-hoc networks history and future development arenas. ITEE J. (2013).

[14] A. A. Celes and N. E. Elizabeth, "Verification Based Authentication Scheme for Bogus Attacks in VANETs for Secure Communication," 2018 International Conference on Communication and Signal Processing (ICCSP), Chennai, 2018, pp. 0388-0392. doi: 10.1109/ICCSP.2018.8524540

[15] K. M. A. Alheeti, A. Gruebler and K. D. McDonald-Maier, "An intrusion detection system against malicious attacks on the communication network of driverless cars," 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, 2015, pp. 916-921. doi: 10.1109/CCNC.2015.7158098

[16] R. Shringar Raw, M. Kumar and N. Singh, "Security Challenges, Issues and Their Solutions For Vanet", International Journal of Network Security & Its Applications, vol. 5, no. 5, pp. 95-105, 2013.

[17] H. Doumenc, “Estudio comparativo de protocolos de encaminamiento en redes vanet,” tech. rep., Universidad Politecnica de Madrid, 2008.

[18] C. Campolo, A. Molinaro, & R. Scopigno (Eds.), Vehicular ad hoc Networks: standards, solutions, and research (Springter Int., 2015).

[19] Currie, Roderick. T. Hacking the CAN Bus: Basic Manipulation of a Modern Automobile Through CAN Bus Reverse Engineering, SANS Institute paper, Mayo 2017.

[20] Schmittner, C., Ma, Z., Reyes, C., Dillinger, O., Puschner, P.: Using SAE J3061for automotive security requirement engineering. In: Skavhaug, A., Guiochet, J.,Schoitsch, E., Bitsch, F. (eds.) SAFECOMP 2016. LNCS, vol. 9923, pp. 157–170.Springer, Cham (2016).https://doi.org/10.1007/978-3-319-45480-113.

Seguridad en Protocolos de Comunicación: Eventos

1st Alejandro Padrón-Godínez
Instrumentación. Científica e Industrial, ICAT- Coordinación de Óptica
UNAM - INAOE
Circuito Exterior S/N CDMX - Tonantzintla, Puebla - México
apadron@inaoep.mx

***Resumen*—En este trabajo presento el diseño e implementación de protocolos de comunicación con el uso técnicas criptográficas, construyendo supuestos eventos donde puede haber vulnerabilidades. Una vez identificado el evento propuesto se pueden diseñar los pasos a seguir en cada caso, además de aplicar los servicios y mecanismos que nos ayudarán a salvar dificultades ante ataques.**

***Palabras Clave*—criptografía, protocolos, servicios y mecanismos de seguridad**

I. Introducción

Los protocolos no deben ser vistos solo como una serie de pasos a seguir como si fuera un recetario, esto no funciona. Los protocolos son una serie de pasos a seguir por varias entidades con tareas individuales para su implementación. Las tareas que deben de realizar las entidades son desde generar claves hasta implementar algoritmos criptográficos en *hardware* o *software* (mecanismos de seguridad) y muchos otros como verificación de datos recibidos. El protocolo debe ser completado; debe haber una acción determinada para cada situación posible. El propósito de los Protocolos.- en la vida cotidiana, hay protocolos informales para casi todo: pedir mercancías por teléfono, jugar al poker, votar en una elección. Nadie piensa mucho acerca de ellos, han evolucionado con el tiempo y digamos todo el mundo sabe cómo usarlos, funcionan razonablemente bien. En estos días, la interacción humana ocurre por redes informáticas en lugar de cara a cara. Las computadoras necesitan protocolos formales para hacer las mismas cosas que la gente hace sin pensar. Muchos protocolos cara a cara se llevan a cabo en presencia del pueblo por ejemplo las votaciones, para garantizar la equidad y la seguridad [1]. Por otro lado la finalidad de la criptografía es resolver problemas de seguridad como no repudio, autenticación, integridad y confidencialidad. En realidad, ese es el punto principal que buscan los computólogos — algo que mucha gente tiende a olvidar. Cualquiera puede aprender todo sobre algoritmos criptográficos y técnicas, pero éstos son de carácter académico al menos que puedan resolver un problema real. Por esta razón vamos a estudiar algunos eventos propuestos para implementar la seguridad en protocolos de comunicación.

II. Seguridad Informática

Las comunicaciones se limitaban a un acceso a la red federal de microondas, en ese entonces como ahora para lograr enlaces seguros se han desarrollado más y mejores protocolos de comunicación segura rápida y eficiente lo que nos lleva a pensar en el desarrollo de esta valiosa herramienta como un valor agregado. Existen diversos protocolos de comunicación que se manejan indistintamente en diferentes medios de comunicación, pero sin la seguridad que se requiere, ya que se pude alterar, borrar y/o modificar la información, o que simplemente no lleguen a su destino [2].

PASPA-DGAPA-UNAM beca de doctorado.

II-A. Lenguaje común: definiciones

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la mejor manera posible. Además que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas dentro de los límites de su autorización [3].

II-B. Servicios de Seguridad

En la actualidad hablamos de seis servicios de seguridad que se manejan para el intercambio de información mediante un protocolo de comunicación: confidencialidad, integridad, autenticidad, disponibilidad, no repudio y control de acceso. No es posible implementarlos todos pero si se pueden implementar algunos gracias a los mecanismos de seguridad que han sido desarrollados hasta ahora. Además no todas las aplicaciones o comunicaciones requieren necesariamente los mismos servicios de seguridad. Los servicios hacen que se resuelvan ciertos problemas del protocolo o que se produzca cierto resultado [4]. Los servicios de seguridad responden a varias incógnitas que se han propuesto en la comunicación y transmisión de información a través de canales que son promiscuos e inseguros, ver la Figura(1).

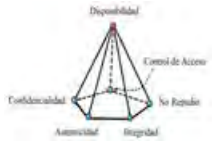


Figura 1. Piramide pentagonal de los servicios de seguridad.

III. Construcción de Protocolos

Un protocolo de comunicación o de red es un acuerdo entre dos o más partes para realizar una tarea específica, una serie de pasos bien definidos y todas las partes involucradas

conocen estos pasos y están de acuerdo en seguirlos. Además un protocolo define claramente lo que cada parte gana o expone con su ejecución. Existen varios tipos de protocolos entre los cuales se mencionan los arbitrados, los adjudicados y los autoimplementados [1].

III-A. Implementación de protocolos

Los protocolos son reglas de comunicación que permiten el flujo de información entre computadoras distintas que manejan lenguajes distintos, por ejemplo, dos computadores conectados en la misma red pero con protocolos diferentes no podrían comunicarse jamás. Para ello, es necesario que ambas "hablen" el mismo idioma, por tal sentido, el protocolo TCP/IP fue creado para las comunicaciones en Internet. Para que cualquier computador se conecte a Internet, es necesario que tenga instalado este protocolo de comunicación. Pueden estar implementados bien en *hardware* (tarjetas de red), *software* (drivers), o una combinación de ambos.

III-A1. Protocolos Arbitrados: Están basados en una tercera parte confiable: el árbitro no tiene ningún tipo y forma de preferencia por ninguna de las partes, en la vida real es el papel que debe jugar un juez. Este tipo de protocolo es poco práctico, por la dificultad de tener una tercera parte confiable y neutral. Objetivo: Alice y Bob hacen compra/venta de un auto usando a S como árbitro.

- 1) A entrega los papeles y las llaves del auto a S
- 2) B entrega el cheque a A.
- 3) A deposita en cheque en el banco
- 4) Si el cheque es bueno, S entrega los papeles y las llaves del auto a B. Si el cheque es malo, S regresa los papeles y las llaves del auto a A. Desde luego, en caso de que el cheque sea malo, A tiene que mostrar pruebas de ello a S.

III-A2. Protocolos Adjudicados: Estos son una variante de los arbitrados y están basados en una tercera parte confiable, pero esta parte no siempre se requiere. Si todas las partes respetan el protocolo, el resultado se logra sin ayuda de la tercera parte denominada adjudicador o tercero en discordia. Si una de las partes involucradas piensa o cree que las otras partes hacen trampa: se invoca al adjudicador como ayuda y el adjudicador analiza la disputa y las reglas además dice quién está actuando bien y qué es lo que se debe hacer. Juzgar la disputa no siempre es sencillo: dependen de la calidad de las evidencias y es tarea del protocolo producir buenas evidencias. Mismo objetivo anterior:

- 1) A entrega llaves y papeles del auto a B.
- 2) B entrega el cheque a A.
- 3) Si el cheque no es bueno, o si los papeles son falsos, A y B comparecen ante un juez y ambos presentan sus evidencias.
- 4) El juez dictamina las evidencias y la parte que engaña es penalizada.

III-A3. Protocolos Autoimplementados: Son los mejores protocolos, se diseñan de tal manera que hacen virtualmente imposible el engaño. No requieren ni árbitro ni juez y garantizan que si cualquier participante engaña, el engaño es descubierto de inmediato por el otro u otros participantes. Propiedades Típicas:

- Detección de la conexión física sobre la que se realiza la conexión (cableada o sin cables)
- Pasos necesarios para comenzar a comunicarse (Handshaking)
- Negociación de las características de la conexión.
- Cómo se inicia y cómo termina un mensaje.
- Formato de los mensajes.
- Qué hacer con los mensajes erróneos o corruptos (corrección de errores)
- Cómo detectar la pérdida inesperada de la conexión, y qué hacer en ese caso.
- Terminación de la sesión de conexión.
- Estrategias para asegurar la seguridad (autenticación, cifrado).

Esta propiedad del protocolo es la que implementaremos en algunos eventos de este trabajo mediante servicios de seguridad y se puede realizar la comprobación de las secuencias pseudoaleatorias utilizando los postulados de Golomb [5].

IV. Circunstancias en donde implementar los protocolos

Ahora se debe analizar el escenario donde se debe establecer la comunicación y qué tipo de servicio de seguridad será necesario implementar en el diseño del protocolo. Para esto veamos primero unos simples desarrollos para entender la notación a utilizar. Partimos de un sistema de comunicación entre Alice y Bob como comúnmente se muestra en la Figura (2), donde también hay un guardián del canal de comunicación.

Figura 2. Esquema de comunicación entre dos partes, guardián y mensaje.

- Luego si las claves $K_A = K_B$ entonces se usará criptografía simétrica de clave secreta o criptografía clásica convencional.
- Si las claves $K_A \neq K_B$ entonces se usará criptografía asimétrica de clave pública.
- Si no hay llave entonces se usarán las funciones Hash o huellas digitales del mensaje.

Ahora denotando la nomenclatura a emplear:

- m: mensaje a transmitir
- m': mensaje recibido a comparar
- A: Alice
- B: Bob
- I: Wendy (atacante o interceptor del mensaje)
- H: Función Hash
- K_a: clave de Alice
- K_b: clave de Bob
- K_{ab}: clave común de Alice y Bob

- vh: valor Hash
- K_a^{pub}: clave pública de Alice
- K_a^{priv}: clave privada de Alice
- K_b^{pub}: clave pública de Bob
- K_b^{priv}: clave privada de Bob
- E: algoritmo de cifrado
- D: algoritmo de descifrado
- C: criptograma
- F: firma digital

AES: algoritmo criptográfico simétrico (Advanced Encryption Standar) NIST, FIPS-197", (2001) [b6].
CBC: modo de operación (cipher block chaining). NIST Special Publication 800-38ª, (2001) [7].
RSA: algoritmo criptográfico asimétrico. Rivest R. et Al., (1978) [8].
MAC: código para autenticación de mensaje. Barak Boaz, (2006) [9].
Algoritmo de Diffie and Hellman para el acuerdo de clave, (1975) [10].

IV-A. Primer Evento

Alice y Bob desean acordar una llave secreta K_s para poder enviarse mensajes cifrados con un "protocolo autoimplementado" garantizando una autenticación unilateral. Un protocolo autoimplementado se diseña de tal manera que se hace virtualmente imposible el engaño y no requieren ni árbitro ni juez. Garantiza que si cualquier participante engaña, el engaño es descubierto de inmediato por el otro u otros participantes. Con esto se implementará el servicio de confidencialidad en el protocolo. Establecido el evento en que se debe desarrollar el protocolo de comunicación sus pasos a seguir serán:

- 1. A: genera la llave secreta K_s.
- 2. A: convierte la llave secreta K_s en una secuencia binaria.
- 3. A: usa criptografía asimétrica para cifrar la llave secreta K_s firmada de acuerdo a: $E_{K_B^{pub}}(E_{K_A^{priv}}(K_s)) = E_{K_B^{pub}}(firma) = C_1$
- 4. A: cifra con la llave secreta K_s un mensaje y obtiene: $E_{K_s}(m_A) = C_2$
- 5. A: envía a B los resultados de C_1 y C_2.
- 6. B: descifra C_1 de acuerdo a: $D_{K_B^{priv}}(C_1) = (firma)$
- 7. B: verifica la firma mediante: $D_{K_A^{pub}}(D_{K_A^{priv}}(K_s)) = D_{K_A^{pub}}(firma) = K_s$
- 8. B: descifra C_2 con la llave secreta y obtiene el mensaje que A le envío: $D_{K_s}(C_2) = m_A$

Este protocolo funciona y es confiable porque nadie más que A y B conocen la llave secreta K_s. Por tanto, nadie más puede leer el mensaje *m* y se acuerda de manera segura la llave.

IV-B. Segundo Evento

En este evento se emplearán los términos de Capa de Conexión Segura (por sus siglas en inglés *Secure Locker Layer*), que es un protocolo criptográfico empleado para realizar conexiones seguras entre un cliente y un servidor. Las suposiciones de este evento son las siguientes:
SLL: genera y distribuye claves de sesión.
SLL: es confiable, emplea criptografía simétrica, caso particular el algoritmo AES-256 bits.
SLL: tiene claves simétricas con Alice (K_{sA}) y clave con Bob (K_{sB}).
Objetivo.- Alice y Bob acuerdan claves K_s a través del servidor de claves.

- 1. A envía SLL: $E_{K_{sA}}$ (requeridas por A, B)=C
- 2. SLL: genera K_s
- 3. SSL: $E_{K_{s_A}} = C_A$
- 4. SLL: $E_{K_{s_B}(K_s)} = C_B$
- 5. SLL envía A: C_A, C_B
- 6. SLL: $D_{K_{s_B}}(C_A) = K_s$
- 7. A envía B: C_B
- 8. B: $D_{K_{s_B}}(C_B) = K_s$

Si agregamos Autenticación mutua con Hand Shake y Verificación de la Integridad tendremos al siguiente protocolo:

- 1. A envía SLL: $E_{K_{sA}}$ (requeridas por A, B)=C
- 2. SLL: genera K_s
- 3. SLL: $E_{K_{sA}}(K_s) = C_A$
- 4. SLL: $E_{K_{sA}^{CBC}}(K_{sB}) = C^A_{MAC-256}$
- 5. SLL: $E_{K_{sB}}(K_s) = C_B$
- 6. SLL: $E_{K_{sB}^{CBC}}(K_{sA}) = C^B_{MAC-256}$
- 7. SLL envía A: $(C_A, C_B, C^A_{MAC-256}, C^B_{MAC-256})$
- 8. A: $D_{K_{sA}}(C_A) = K_s$
- 9. A: $D_{K_{sA}^{CBC}}(C^A_{MAC-256}) = K_{s_B}$
- 10. A: $D_{K_{sB}}(C_B) = K_s$
- 11. A envía B: $(C_A, C_B, C^A_{MAC-64}, C^B_{MAC-256})$
- 12. B: $D_{K_{sB}}(C_B) = K_s$
- 13. B: $D_{K_{sB}^{CBC}}(C^B_{MAC-256}) = K_{s_A}$
- 14. B: $D_{K_{sA}}(C_A) = K_s$
- 15. B: $D_{K_s}(K_{sB}) = C_1$
- 16. B envía A: C_1
- 17. A: $D_{K_s}(C_1) = K_{s_B}$

IV-C. Tercer Evento

Veamos las suposiciones para este caso:
- Alice tiene el documento que desea transmitir.
- Se usará el algoritmo RSA para firmar y verificar (criptografía asimétrica).
- Todas las claves K están certificadas.
- Todas las partes tienen sus propias parejas de claves (púbica y privada).
- AC: Autoridad Certificadora, es confiable además verifica todas las firmas.

Objetivo.- A, B y C deben firmar el documento *m* y AC debe verificar todas y cada una de las firmas.

- 1. A: $F^{priv}_{K_A}(m) = s_A$
- 2. A envía $B : (s_A, m)$
- 3. B: $F^{priv}_{K_B}(m) = s_B$
- 4. B envía C: (s_A, s_B, m)
- 5. C: $F^{priv}_{K_C}(m) = s_C$
- 6. C: envía AC: (s_A, s_B, s_C, m)
- 7. AC:$v^{pub}_{K_A}(S_A) = m$, $v^{pub}_{K_B}(S_B) = m$, $v^{pub}_{K_C}(S_C) = m$.

Si se agregará Confidencialidad y Verificación de la Integridad el protocolo quedaría como:

- 1. A: $H_A(m) = vh_A$
- 2. A: $E^{pub}_{K_{AC}}(F^{priv}_{K_A}(m, vh_A)) = s^{H_A(m)}_A$
- 3. A envía B $(s^{H_A(m)}_A, m)$
- 4. B: $H_B(m) = vh_B$
- 5. B: $E^{pub}_{K_{AC}}(F^{priv}_{K_B}(m, vh_B)) = s^{H_B(m)}_B$
- 6. B envía C:$(s^{H_A(m)}_A, s^{H_B(m)}_B, m)$
- 7. C: $H_C(m) = vh_C$
- 8. C: $E^{pub}_{K_{AC}}(F^{priv}_{K_C}(m, vh_C)) = s^{H_C(m)}_C$
- 9. C envía AC:$(s^{H_A(m)}_A, s^{H_B(m)}_B, s^{H_C(m)}_C, m)$
- 10. AC: $D^{priv}_{K_{AC}}(v^{pub}_{K_A}(s^{H_A(m)}_A)) = m, vh_A$
  AC: $H_A(m) = vh'_A$
  AC: $vh_A = vh'_A$
- 11. AC: $D^{priv}_{K_{AC}}(v^{pub}_{K_B}(s^{H_B(m)}_B)) = m, vh_B$
  AC: $H_B(m) = vh'_B$
  AC: $vh_B = vh'_B$
- 12. A$D^{priv}_{K_{AC}}(v^{pub}_{K_C}(s^{H_C(m)}_C)) = m, vh_C$
  AC: $H_C(m) = vh'_C$
  AC: $vh_C = vh'_C$

Ahora se le agrega la fecha y la hora al protocolo:

- 1. A:$F^{priv}_{K_A}(m) = s^m_A$
- 2. A:$F^{priv}_{K_A}(TS_A) = s^{TS_A}_A$
- 3. A envía B: $(s^m_A, s^{TS_A}_A, m)$
- 4. B:$F^{priv}_{K_B}(m) = s^m_B$
- 5. B:$F^{priv}_{K_B}(TS_B) = s^{TS_B}_B$
- 6. B envía C: $(s^m_A, s^{TS_A}_A, s^m_B, s^{TS_B}_B, m)$
- 7. C: $F^{priv}_{K_C}(m) = s^m_C$
- 8. C: $F^{priv}_{K_C}(TS_C) = s^{TS_C}_C$
- 9. C envía AC:$(s^m_A, s^{TS_A}_A, s^m_B, s^{TS_B}_B, s^m_C, s^{TS_B}_B, s^m_C, s^{TS_C}_C, m)$
- 10. AC:
  $v^{pub}_{K_A} s_A = m, v^{pub}_{K_A}(s^{TS_A}_A) = TS_A$
  $v^{pub}_{K_B} s_B = m, v^{pub}_{K_B}(s^{TS_B}_B) = TS_B$
  $v^{pub}_{K_C} s_C = m, v^{pub}_{K_C}(s^{TS_C}_C) = TS_C$

IV-D. Cuarto Evento

Para este evento de estudio vamos a implementar una Autenticación Mutua y Verificación de Integridad bajo las consideraciones que se mostraron en el caso de estudio IV-C, inmediato anterior. También para este estudio se emplearán tanto técnicas de criptografía simétrica como pública, en particular los algoritmos son el AES de 256-bits y RSA de 2048 respectivamente. Para empezar nuestro protocolo del evento citado veamos como empleamos los algoritmos de cifrado:

- 1. A: genera K_s
- 2. A: $E^{AES}_{K_s}(m) = C_1$
- 3. A: $E_{RSA^{pub}_{K_B}}(E_{RSA^{priv}_{K_sA}}(K_s)) = C_2$
  donde $E_{RSA^{priv}_{K_A}}(K_s)$ es la firma
- 4. A envía B: C1, C2
- 5. B: $E_{K^{priv}_B}(C_2)) = Firma$
- 6. B: $D_{K^{pub}_A}(E^{priv}_{K_A}(K_s)) = K_s$
- 7. $D^{AES}_{K_s}(C_2) = m$

Ahora vamos a implementar la Confidencialidad y Autenticación mutua:

- 1. A: $E_{K_{ab}}(m) = C_1$
- 2. A envía B: C_1
- 3. B: $D_{K_{ab}}(C_1) = m$
- 4. B: $E_{K_{ab}}(m') = C_2$
- 5. B envía A: C_2
- 6. A: $D_{K_{ab}}(C_2) = m'$
- 7. A: m'=m, compara

Si le sumamos Integridad al protocolo anterior se obtiene:

- 1. A: $E_{K_{ab}}(m) = C_1$
- 2. A: $E_{K^{CBC}_{ab}}(m) = C^A_{MAC-256}$
- 3. A envía B:$(C_1, C^A_{MAC-256})$
- 4. B: $D_{K_{ab}}(C_1) = m'$
- 5. B: $E_{K^{CBC}_{ab}}(m) = C^B_{MAC-256}(')$
- 6. B: $C^B_{MAC-256}(') = C^B_{MAC-256}$ compara
- 7. B envía A: $(C^B_{MAC-256}('), m')$
- 8. A: $E_{K^{CBC}_{ab}}(m') = C^A_{MAC-256}$
- 9. A: $C^A_{MAC-256} = C^A_{MAC-256}(')$ compara

V. Conclusiones

Se presentaron varios desarrollos de seguridad en protocolos de comunicación implementando servicios y mecanismos de seguridad que nos ayudan a salvar vulnerabilidades y riesgos ante atacantes. Se han presentado cuatro eventos como casos de estudio para la implementación de protocolos seguros, que si bien sus estructuras son conocidas a veces no se sabe cuando, como y donde implementarlas. La confidencialidad, integridad, autenticidad dentro de protocolos se pueden garantizar de manera confiable mediante técnicas de Criptografía. La relevancia es la factibilidad técnica y eficiencia de los protocolos, al implementarlos ya sea en *software* o *hardware* dentro los protocolos que usamos para sistemas de comunicación y que pueden ser usados en otras aplicaciones.

Referencias

[1] Schneier B., "Applied Cryptography", John Wiley and Sons, Inc., EUA. (1996).

[2] Daltabuit E., Hernández L., Mallén G., Vázquez J., "La seguridad de la Información," Ed. Limusa, 2007.

[3] Menezes A., Oorschot P. V and Vanstone S. "Handbook of Applied Cryptography", CRC Press, (1997).

[4] INTERNATIONAL STANDARD, ISO 7498-2, "Information processing - Open Systems Interconnection - Basic Reference Model. Security Architecture," First edition 1989-02-15.

[5] Golomb S. W. Shift Register Sequences, Prentice Hall Inc. EUA. , (1967).

[6] NIST, "Federal Information Processing Standards Publication 197", ADVANCED ENCRYPTION STANDARD (AES), November 26. (2001).

[7] NIST Special Publication 800-38ª, "Recommendation for block cipher modes of operation", (2001).

[8] Rivest R., Shamir A., Adleman L., (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM, Vol. 21 (2), pp.120–126. Previously released as an MIT "Technical Memoïn April 1977. Initial publication of the RSA scheme.

[9] Barak Boaz, "Computer Science 433 Cryptography", Princeton University Computer Science Department. (2006).

[10] Diffie W., Hellman M. E. "New Directions in Cryptography", IEEE Information Theory Workshop, Lenox, MA, EUA. (1975).

Índice de Autores