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.

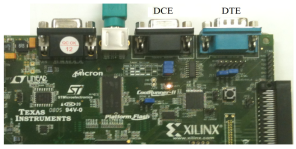

Figura 1. Spartan 3E con dos puertos seriales.

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

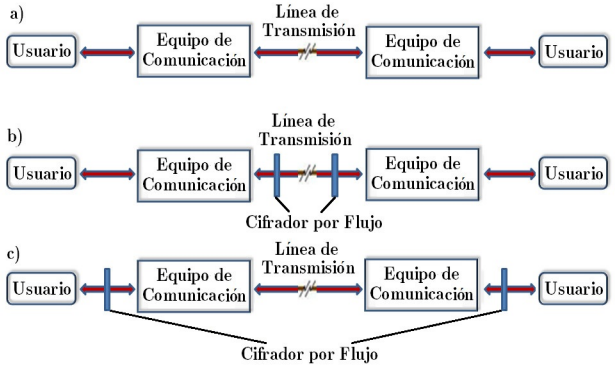

Figura 2. Diagrama de bloques de un sistema de comunicación simplificado. a) Sistema Inseguro. b) Sistema con el cifrado en los extremos de la línea de la transmisión. c) Sistema con el cifrado como interfaz entre el usuario y el equipo de comunicación.

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

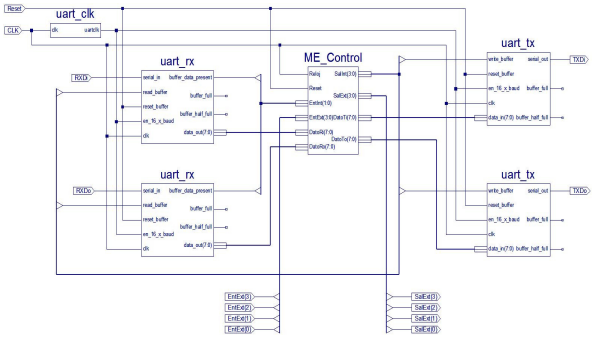

Figura 4. Diseño de la Plataforma integrando el bloque de control.

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

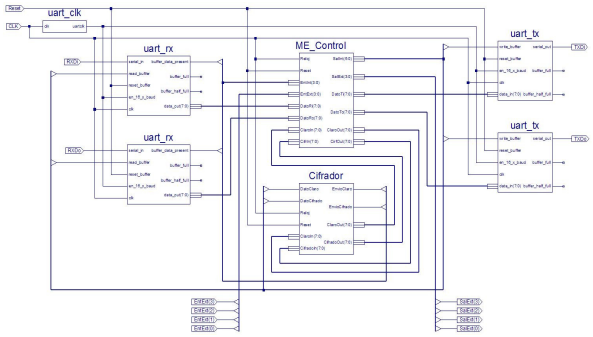

Figura 5. Diseño de la Plataforma Criptográfica incorporando el proceso de cifrado/descifrado como un bloque independiente.

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

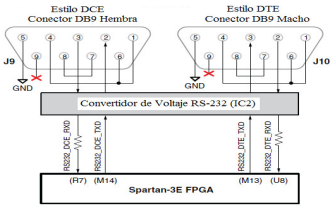

Figura 6. Puertos Seriales RS-232.

- $RS-232\_DCE\_TXD$ 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).

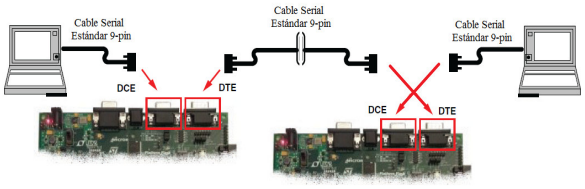

Figura 7. Esquema de conexiones para la plataforma criptográfica.

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

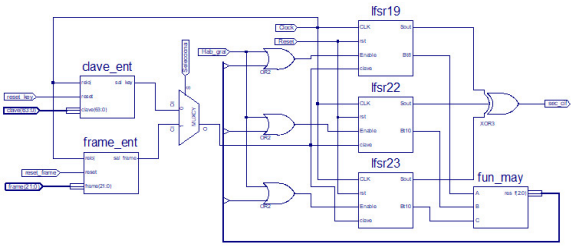

Figura 8. Implementación del algoritmo A5_1.

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).