Diseño y Desarrollo de una Plataforma Criptográfica Reconfigurable de Alto Desempeño

Ignacio Algredo-Badillo, René Cumplido-Parra, Claudia Feregrino-Uribe

[1] Instituto Nacional de Astrofísica, Óptica y Electrónica, INAOE, Coordinación de Ciencias Computacionales,
Luis Enrique Erro #1, CP 72840, Sta. Ma. Tonantzintla, Puebla, México.
talion00z@ccc.inaoep.mx, {rcumplido,cferegrino}@inaoep.mx

Abstract. This work reports on the design and development of a reconfigurable cryptographic platform, which handles a configuration library that can be modified and extended by the user. Several approaches were implemented and the one with higher performance during the information processing was select as the best approach. The motivation for this work is the necessity of freeing the communication networks of at least 1 Gbps from the information traffic and the ability to handle several cryptographic standards to increase the security in a case a standard expires, emerges or presents some weakness. We have used a hardware system with reconfigurable architecture for its inherent advantages on reconfiguration and because of the usual better performance of hardware implementations rather than software ones.

Resumen. Este trabajo reporta el diseño y desarrollo de una plataforma criptográfica reconfigurable, la cual maneja una biblioteca de configuraciones que puede ser modificada y extendida. Se realizó un análisis de desempeños y módulos utilizados para seleccionar el enfoque del esquema arquitectural que tuviera un alto desempeño en el procesamiento de información. Las motivaciones se deben a la necesidad de descongestionar el tráfico de información en las redes de comunicación para velocidades de transferencia de al menos 1 Gbps y la habilidad de manejar diversas implementaciones de algoritmos criptográficos para aumentar la seguridad si un estándar caduca, aparece o presenta una debilidad. Se utiliza un sistema hardware con arquitectura reconfigurable por las ventajas inherentes de la reconfiguración y que generalmente las implementaciones algorítmicas en hardware tienen mejor desempeño que las implementaciones en software.

Palabras Clave: FPGA, algoritmos criptográficos, cómputo reconfigurable.

1 Introducción

En la actualidad, se presentan varios problemas de seguridad en las redes de comunicación, existiendo distintas formas de solventarlos. Una manera es utilizar criptografía para ofrecer confidencialidad, integridad, control de acceso y autenticación, dependiendo del algoritmo cifrador. Algunos protocolos de

comunicación hacen uso de una variedad de estándares criptográficos, por lo que es necesario un sistema que maneje implementaciones criptográficas que puedan ser modificadas, alternadas, extendidas y agregadas. Esto aumenta la seguridad, ya que los estándares pueden llegar a ser caducos o débiles, aunado a que pueden aparecer nuevos estándares criptográficos. La desventaja de usar criptografía en las redes de comunicación es que el cálculo implícito en las implementaciones cifradoras congestiona el tráfico de información, necesitándose implementaciones que tengan un desempeño alto.

La plataforma presentada en este trabajo tiene un diseño basado en el cómputo reconfigurable debido a las características que provee para manejar distintas implementaciones sobre dispositivos hardware configurables como los arreglos de compuertas programables (FPGAs, *Field Programmable Gate Arrays*). Con lo anterior y de manera general, las implementaciones algorítmicas en hardware tienen un mejor desempeño que las implementaciones en software que tienen el mismo grado de seguridad, además de su capacidad para proteger llaves privadas del acceso de intrusos, aunque las arquitecturas software pueden ser soportadas en múltiples plataformas hardware [1].

El diseño de la plataforma se basó en un análisis para la selección de su enfoque arquitectural. El análisis se fundamentó en las implementaciones de diseños modulares de los algoritmos DES, AES, SHA-1 y MD5, las cuales aportaron información para seleccionar el nivel de reconfiguración del sistema y la arquitectura que presentará un mayor rendimiento. Existen varios estándares para establecer la velocidad de transferencia de información y el Giga-Ethernet es uno de los más importantes y rápidos, el cual trabaja transmitiendo datos a un gigabit por segundo.

Uno de los protocolos de comunicación que se usan en las redes Giga-Ethernet es IPSec, que además provee de seguridad sin depender de un algoritmo criptográfico en particular, ya que los estándares criptográficos se definen al momento de establecer la comunicación.

1.1 Algoritmos criptográficos

La criptografía es la técnica o camino de la escritura secreta [2]. El principio básico de la criptografía es mantener la privacidad de la comunicación entre dos personas alterando el mensaje original de modo que sea incomprensible a toda persona distinta del destinatario, además de que un tercero no pueda hacerse pasar por el emisor.

Existe una gran cantidad de algoritmos criptográficos, por lo que se tienen diferentes clases dependientes de su utilidad [3], ver tabla 1.

La plataforma criptográfica reconfigurable consta de una biblioteca de configuraciones de implementaciones criptográficas, la cual se desea que tenga diseños de alto desempeño de una gran cantidad de estándares cifradores. Debido a la gran cantidad de algoritmos criptográficos, se seleccionó un conjunto inicial de estándares utilizados en IPSec para implementarlos. Se escogió al algoritmo DES por su amplia difusión, al AES por su reciente aparición y a los estándares SHA-1 y MD5 por ser funciones resumen (*hash*) útiles en IPSec.

Tabla 1. Clases de algoritmos criptográficos

Algoritmo	Confidencialidad	Autenticación	Integridad	Intercambio de llaves
Simétrico	✓	×	×	✓
Asimétrico	✓	×	×	✓
Firma digital	×	✓	✓	×
Intercambio de llaves	✓	Opcional	×	✓
Funciones resumen	×	×	✓	×
Códigos de autenticación	×	✓	✓	×

Las implementaciones de dichos algoritmos debe tener un desempeño igual o mayor a un gigabit por segundo para poder ser utilizados en redes Giga-Ethernet.

1.2 Cómputo reconfigurable

Las soluciones hardware convencionales ofrecen un excelente desempeño, pero no tienen la flexibilidad de las soluciones software. Además, si se utilizaran varios circuitos integrados de aplicación específica (ASICs) para tener un sistema con varias funcionalidades criptográficas, se desperdiciarían recursos económicos y de área, por lo que es favorable utilizar un dispositivo que pueda ser reconfigurado y no sean malgastados los recursos. Los FPGAs ofrecen la posibilidad de manejar la reconfiguración, es decir, cambiar su funcionalidad con respecto al tiempo. Potencialmente, el cómputo reconfigurable tiene un comportamiento más eficiente que el cómputo en software, mientras mantiene una mayor flexibilidad que el cómputo en hardware [4].

El cómputo reconfigurable tiene el potencial de cambiar la forma en que se realiza el cómputo, ya que maneja las ventajas del cómputo espacial como el manejo de bloques funcionales especializados y paralelismo, así como las ventajas del cómputo temporal para reutilizar recursos de hardware. En resumen, las ventajas de los FPGAs utilizando cómputo reconfigurable se pueden ver en la figura 1.

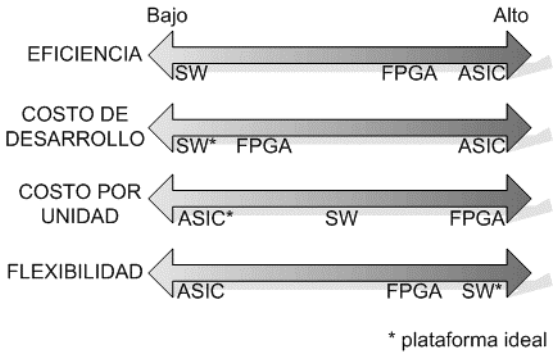

Fig. 1. Ventajas del uso de dispositivos FPGAs con diseños basados en el cómputo reconfigurable, sobre dispositivos software (por ejemplo procesadores) y ASICs

2 Trabajo relacionado

La búsqueda de trabajos relacionados se basó en implementaciones de arquitecturas reconfigurables, con funciones para el procesamiento criptográfico. Las características a comparar son los algoritmos implementados y el desempeño resultante.

CryptoManiac [5] es un procesador que consiste básicamente de cuatro unidades funcionales operando en una memoria de datos común, con una arquitectura de 4 estados de segmentación. La tabla 2 muestra el desempeño de una configuración para varias implementaciones criptográficas de CryptoManiac con una frecuencia de reloj de 360Mhz.

Tabla 2. Desempeño de implementaciones criptográficas en el procesador CryptoManiac trabajando a una frecuencia de reloj de 360 MHz

Algoritmo	Total de ciclos	Desempeño (Mbps)
3DES	336 (7 ciclos * 48)	68
3DES corr.	392 (7 ciclos * 56)	59
AES – 128/128	90 (9 ciclos *10)	511
AES – 128/128 corr.	130 (9 ciclos *13)	353

En [6] se reporta Cryptonite, un procesador que no ha sido construido en realidad y los resultados de este trabajo de investigación son basados en simulación de software y resultados de síntesis de elementos de hardware. El autor está consciente de que sus mediciones no han sido realizadas en hardware real y en la tabla 3 se muestran los resultados de simulaciones de algunos algoritmos criptográficos utilizando este procesador.

Tabla 3. Desempeño de implementaciones criptográficas en el procesador Cryptonite trabajando a una frecuencia de reloj de 400 MHz

Algoritmo	Total de ciclos	Desempeño (Mbps)
AES – 128/128	80	640
AES – 128/128	70	732
DES	35	732
3DES	105	244
MD5	504	406
SHA-1	488	420

En el trabajo [7] se tiene la implementación de los algoritmos Crypton, IDEA, RC6 y Twofish en un sistema reconfigurable denominado PipeRench, el cual maneja un sistema de reconfiguración con diseño segmentado y hardware virtual donde implementaciones de gran tamaño pueden correr en hardware limitado físicamente. Los algoritmos criptográficos son diferentes a los implementados en este trabajo, pero

el Twofish es la implementación que alcanza la más alta velocidad de procesamiento, 164.7 Mbps.

Cobra [8] es una arquitectura reconfigurable especializada con mejor flexibilidad que los ASICs o las soluciones programables como procesadores, además tiene tiempos rápidos de reconfiguración. Se reporta un análisis para obtener un esquema básico de elementos de procesamiento comunes y un grupo especial de elementos reconfigurables para obtener una funcionalidad criptográfica deseada. Fueron implementados RC6, Rijndael y Serpent en VHDL, pero los resultados de implementación son comparados entre los números de ciclos que tardan en cifrar un bloque para cada algoritmo. La arquitectura Cobra se desarrolló en base a un modelo híbrido de una arquitectura reconfigurable para el aceleramiento de las implementaciones de los bloques cifradores. La reconfiguración se hace en tiempo de ejecución que establece metas de agilidad del algoritmo y aumenta la eficiencia con respecto a las implementaciones en software. Para la configuración, un ensamblador es necesario para compilar un programa en lenguaje ensamblador hacia el formato del microcódigo COBRA. La arquitectura asegura un total soporte de las operaciones requeridas para un algoritmo maximizando la densidad funcional del bus de datos. Los elementos criptográficos reconfigurables (RCE, *reconfigurable cryptographic elements*) son los bloques básicos de la arquitectura Cobra y operan con bloques de datos de hasta 32 bits.

Los trabajos revisados tienen la característica de reconfiguración para sistemas criptográficos, ofreciendo la flexibilidad y las ventajas de un sistema reconfigurable pero sin resolver problemas de congestionamiento del tráfico de información y/o sin manejar bajas frecuencias de reloj (particularidad que influye directamente con el consumo de potencia). Las arquitecturas reconfigurables revisadas tienen un esquema parecido a un procesador, aunque la arquitectura Cobra tiene un nivel de paralelismo, pero no muy especializado, con un esquema de elementos básicos y elementos reconfigurables que reducen el tiempo necesario para realizar una reconfiguración. El trabajo presentado en este artículo utiliza una arquitectura que reconfigura un módulo con una funcionalidad criptográfica completa por otro módulo, que a diferencia de los trabajos relacionados maneja frecuencias de reloj bajas.

3 Plataforma reconfigurable criptográfica

El desarrollo y diseño de este proyecto se realizó en tres etapas principales:

1. Implementación de diseños modulares de los algoritmos DES, AES, SHA-1 y MD5.
2. Análisis y selección del enfoque de la arquitectura de la plataforma criptográfica reconfigurable.
3. Implementación de algoritmos criptográficos con un desempeño de al menos un gigabit por segundo sobre la plataforma seleccionada.

La selección de esta metodología se llevó a cabo por el nivel de reconfiguración que se requería, ya que se necesitaba tener un sistema reconfigurable con un

desempeño considerable. Al realizarse diseños modulares óptimos en recursos de un conjunto de algoritmos criptográficos, se puede realizar un análisis de los componentes utilizados y conocer si existe un subconjunto de módulos que sea común entre las distintas implementaciones, donde los demás módulos sean reconfigurados para que funcionen como elementos especializados de una determinada Implementación.

Analizar el número de módulos comunes entre los diseños modulares, así como el desempeño de las implementaciones de cada diseño modular, permitió seleccionar el mejor enfoque, de acuerdo al análisis, de la arquitectura reconfigurable criptográfica.

Por último, al tener el enfoque óptimo de la plataforma se procedió a implementar algoritmos con un desempeño mayor a 1 Gbps, los cuales trabajarán sobre la arquitectura reconfigurable seleccionada.

3.1 Etapa 1: Implementaciones modulares

Para realizar el análisis modular para la selección del enfoque de la arquitectura de la unidad de procesamiento, se realizaron implementaciones de los estándares criptográficos seleccionados con diseños modulares.

Los parámetros a medir son el número de componentes comunes entre las implementaciones y conocer el nivel necesario de reconfiguración, así como el desempeño que las implementaciones tienen y poder decidir sobre el enfoque que aumentaría tal procesamiento.

Este punto de vista se basó en que la mayoría de los cifradores pueden ser especificados como flujos de datos en un grafo constituido de pocos componentes [9]. En general, hay ciertos componentes comunes utilizados en el cálculo que realizan los algoritmos criptográficos: operaciones de aritmética simple, multiplicación (de propósito general, por una constante o con esquema de codificación redundante), operaciones lógicas paralelas, secuencias de operaciones lógicas, LUTs (*table lookup*), rotaciones y corrimientos.

Las implementaciones de los algoritmos DES y AES se basaron en los estándares FIPS 46-3 [10] y FIPS 197[11] respectivamente y el diagrama a bloques general se muestra en la figura 2.

Los algoritmos SHA-1 y MD5 se basaron en los estándares FIPS 180-2 [12] y RFC 1321 [13] respectivamente, y el diagrama a bloques general se muestra en la figura 3.

Las implementaciones se realizaron y simularon en Active-HDL 5.1 e implementaron y validaron con el modelo post-implementación de la herramienta Xilinx ISE 6, las cuales tienen un alto desempeño considerando que no utilizan técnicas de diseño para mejorar el rendimiento. Los resultados de estas implementaciones se pueden ver en las tablas 4 y 5.

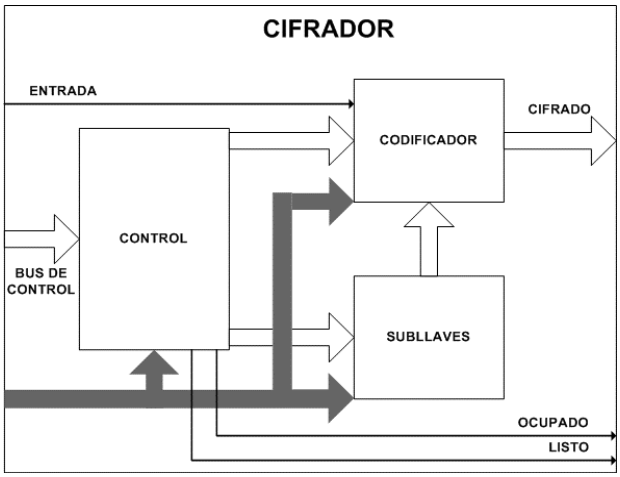

Fig. 2. Diagrama a bloques de las implementaciones de los algoritmos simétricos DES y AES, el cual consta de tres unidades principales: un módulo de control, un módulo de generación de llaves para cada ronda y una unidad codificadora para el cálculo del cifrado.

3.2 Etapa 2: Análisis

Los resultados de la sección 3.1 son de las implementaciones funcionales de los algoritmos criptográficos en base a diseños modulares para seleccionar un enfoque del esquema de reconfiguración, entre los cuales se consideran los siguientes:

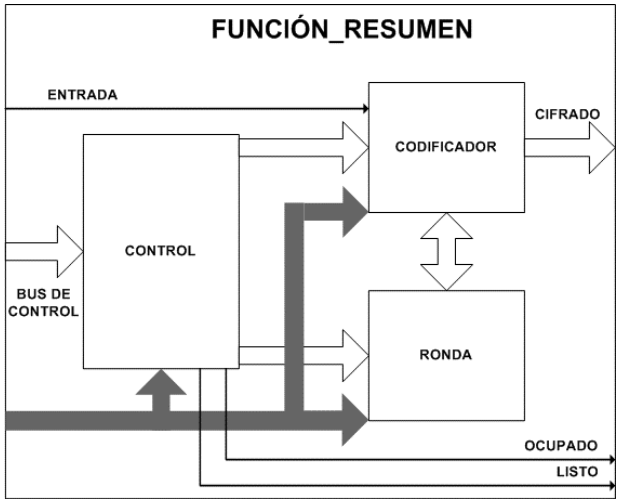

Fig. 3. Diagrama a bloques de las implementaciones de las funciones resumen SHA-1 y MD5, el cual consta de tres unidades principales: un módulo de control, un módulo ronda que actualiza el mensaje de entrada cada ronda y una unidad codificadora para el cálculo del resumen.

Tabla 4. Tipo y cantidad de módulos de las implementaciones

Componente	Descripción	DES	AES	SHA1	AES
AND2TO1_32BIT	AND de 2 entradas 32bits			4	4
NOT_32BIT	NOT de 32 bits			1	2
OR2TO1_32BIT	OR de 2 entradas de 32bits				3
XOR2TO1_8BIT	XOR de 2 entradas de 8 bits		33		
XOR4TO1_8BIT	XOR de 4 entradas de 8 bits		16		
XOR2TO1_9BIT	XOR de 2 entradas de 9 bits		16		
XOR2TO1_32BIT	XOR de 2 entradas de 32 bits	1	1	5	3
XOR3TO1_32BIT	XOR de 3 entradas de 32 bits		1		
XOR4TO1_32BIT	XOR de 4 entradas de 32 bits		1		
XOR5TO1_32BIT	XOR de 5 entradas de 32 bits		1		
XOR2TO1_48BIT	XOR de 2 entradas de 48 bits	1			
XOR2TO1_64BIT	XOR de 2 entradas de 64 bits				
XOR2TO1_128BIT	XOR de 2 entradas de 128 bits		2		
REGISTRO_28BIT	Registro de 28 bits	2			
REGISTRO_32BIT	Registro de 32 bits	2			
REGISTRO_128BIT	Registro de 128 bits		2		
REGISTRO_160BIT	Registro de 160 bits			1	
REGISTRO_512BIT	Registro de 512 bits			1	
SUMADOR2TO1_32BIT	Sumador modulo 2^{32} de 32 bits			9	8
MUX2TO1_8BIT	Multiplexor de 2 entradas de 8 bits		32		
MUX3TO1_28BIT	Multiplexor de 3 entradas de 28 bits	2			
MUX2TO1_32BIT	Multiplexor de 2 entradas de 32 bits	2		1	
MUX3TO1_32BIT	Multiplexor de 3 entradas de 32 bits			1	
MUX4TO1_32BIT	Multiplexor de 4 entradas de 32 bits			1	1
MUX2TO1_128BIT	Multiplexor de 2 entradas de 128 bits		2		1
MUX3TO1_128BIT	Multiplexor de 3 entradas de 128 bits		1		
MUX2TO1_160BIT	Multiplexor de 2 entradas de 160 bits			1	
MUX2TO1_512BIT	Multiplexor de 2 entradas de 512 bits			1	
BLOQUES RAM 64X32	Memoria 64 x 32 bits				1
BLOQUES RAM 64X4	Memoria 64 x 4 bits	8			
BLOQUES RAM 256X8	Memoria 256 x 8 bits		10		
CONTADOR_4BCD	Contador				1
CONTADOR_64BCD	Contador				1
CONTADOR_80BCD	Contador			1	
MEF 7 ESTADOS	Máquina de estados finitos	1			1
MEF 8 ESTADOS	Máquina de estados finitos			1	
MEF 11 ESTADOS	Máquina de estados finitos		1		
MEF 17 ESTADOS	Máquina de estados finitos	1			

Tabla 5. Desempeño de las implementaciones del conjunto inicial de estándares criptográficos

Algoritmo	Total de ciclos	Frecuencia del reloj	Desempeño (Mbps)
DES	17	149.2 MHz	561.72 Mbps
AES	12	86.94 MHz	927.37 Mbps
SHA-1	80	99.44 MHz	636.43 Mbps
MD5	65	51.60 MHz	406.48 Mbps

i. Unidades de Procesamiento Reconfigurables y Unidades de Procesamiento Básicas. Se considera que se tienen unidades de procesamiento comunes a las implementaciones de los algoritmos criptográficos seleccionados, y se tienen

unidades especializadas para realizar el trabajo criptográfico requerido. Estas unidades especiales son elementos reconfigurables del sistema, ya que son útiles y únicas para una implementación y funcionalidad deseada.

ii. Esquema de Bloques Cifradores. Esta plataforma requiere, para obtener una diversidad en su funcionalidad criptográfica, reemplazar totalmente un módulo por otro módulo con una operación criptográfica distinta o con un diseño diferente, por lo que este módulo tiene la característica de reconfigurabilidad.

iii. Sistema con ALU especializada. Este esquema presenta un modo de procesamiento similar a un procesador, pero con una unidad lógica aritmética (ALU) especial para realizar el procesamiento de distintas implementaciones de algoritmos criptográficos. La ALU es el único módulo reconfigurable, cuya operación queda determinada por la función criptográfica a procesar.

El análisis realizado para seleccionar el enfoque se basa en dos partes: el análisis modular y el análisis de desempeños. El primero resuelve el nivel de reconfiguración del esquema, ya que entre mayor sea el nivel de reconfiguración que se utilice, mayor es el tiempo necesario para llevar a cabo la reconfiguración. La segunda parte soluciona el problema de congestionamiento de información. Ambas partes se explican con mayor detalle a continuación.

a.) Análisis Modular. La tabla 4 resalta que los componentes no son comunes entre las diferentes implementaciones criptográficas, a excepción del módulo XOR de 32 bits de dos entradas. Mantener un número mínimo de componentes reconfigurables y básicos no sería un esquema ideal, porque la reconfiguración sería mayor aunado a la conexión que se puede complicar al reutilizar algunos módulos. El esquema con la ALU especializada sería reconfigurada totalmente porque la funcionalidad difiere de la implementación de un algoritmo a otro. Finalmente, el esquema restante consiste en manejar bloques o módulos completos que contienen la lógica necesaria para realizar el procesamiento criptográfico, ya sea de autenticación o de cifrado, por lo que los tiempos de reconfiguración son muy similares pero se tiene un nivel bajo de reconfiguración con el Esquema de Bloques Cifradores.

b.-) Análisis de desempeños. Los desempeños presentados en la tabla 5 son altos debido a las implementaciones completas en el FPGA, por lo que utilizar un esquema de reconfiguración con ALU especializada reduciría la capacidad de procesamiento ya que se manejaría una metodología de implementación algorítmica secuencial, perdiendo la capacidad de paralelismo que acelera el procesamiento de información. Un esquema con bloques básicos y reconfigurables tiene un mejor desempeño, pero éste es relativamente más bajo que el esquema con bloques cifradores completos, ya que aumenta el tiempo del camino crítico lo que reduce el desempeño. El resultado de la segunda parte resalta al enfoque del esquema de bloques cifradores, solventando los problemas y desventajas de los otros esquemas.

El resultado del análisis concluye que el enfoque con bloques cifradores completos (ver figura 4), donde la unidad Bloque Cifrador Reconfigurable cambia su funcionalidad o desempeño al reconfigurarse por otra implementación, satisface las consideraciones para tener un alto desempeño con un tiempo de reconfiguración óptimo.

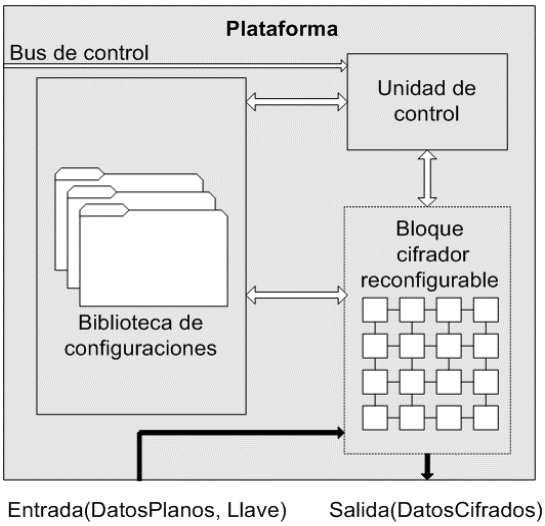

Fig. 4. Esquema con bloques cifradores reconfigurables completos, enfoque seleccionado para la plataforma criptográfica reconfigurable para un alto desempeño y un tiempo de reconfiguración óptimo.

3.2 Etapa 3: Implementación a 1 Gbps

Se han realizado las implementaciones con un desempeño de al menos 1 Gbps para los algoritmos AES, SHA-1 y MD5, mientras que el algoritmo DES, en los últimos diseños implementados, está procesando a 927.37 Mbps con una arquitectura con cuatro rondas desenrolladas. Se siguieron distintas metodologías para la implementación de cada estándar criptográfico, las cuales son descritas a continuación. La técnica de segmentación (*pipeline*) no fue utilizada, lo que se hizo fue replicar lógica de manera completa y parcial, debido a que los modos de funcionamiento como el CBC necesitan el cifrado de un bloque para iniciar el procesamiento del siguiente bloque, además las funciones resumen implementadas en este trabajo, al cifrar mensaje mayores de 512 bits también utilizan el cifrado de un bloque para iniciar el cálculo del siguiente, ver figura 5.

Las técnicas de diseño y los resultados de implementación para un procesamiento de un gigabit por segundo se describen a continuación.

a. AES. La implementación del AES en la sección 3.1 usa 10 bloques de memoria distribuida sobre el FPGA, por lo que se utilizan demasiados recursos del dispositivo tanto para conectar los elementos operacionales como la lógica funcional del proceso AES. El desempeño alcanzado por las primeras implementaciones era cercano al gigabit por segundo, por lo que usar las memorias empotradas de doble puerto del FPGA disminuyó el camino crítico, ya que además de no utilizar lógica distribuida se necesitaron sólo 5 memorias secuenciales de 2 puertos, evitándose también los registros del módulo Codificador (ver figura 2). El desempeño se muestra en la tabla 6.

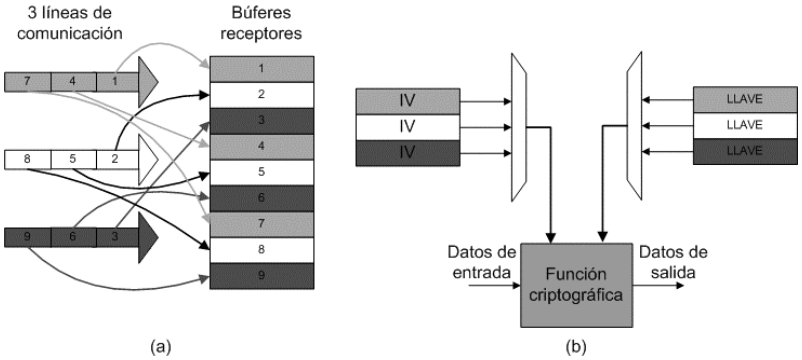

Fig. 5. (a) Uso de diseños segmentados de 3 etapas tienen utilidad en sistemas que manejan 3 líneas de comunicación en IPSec. (b) Una función criptográfica con 3 etapas de segmentación necesita vectores de inicialización y llaves para cada línea de comunicación.

Tabla 6. Desempeño de las implementaciones de los estandares criptográficos

Algoritmo	Total de ciclos	Frecuencia del reloj	Desempeño
AES	10	96.42 MHz	1.451 Gbps
DES	4	49.29 MHz	0.917 Gbps
SHA-1	20	43.30 MHz	1.109 Gbps
MD5	16	32.47 MHz	1.039 Gbps

b. SHA-1. La implementación del algoritmo SHA-1 en la sección 3.1 fue optimizada en el camino crítico al analizar la conexión de 5 sumadores modulares de la unidad Ronda (ver figura 3) y aumentar el desempeño. Esta mejora fue utilizada en un nuevo diseño con rondas parcialmente desenrolladas que aumentaron su desempeño, ver tabla 6.

c. MD5. La nueva implementación del algoritmo MD5 siguió un desarrollo similar que la nueva implementación del algoritmo SHA-1, cuyos resultados no habían logrado un desempeño mayor a 1 Gbps. Se encontró que el ruteo de la lógica aumentaba al usar diseños con rondas parcialmente desenrolladas, afectando el tiempo del camino crítico, por lo que se redujo al implantar nuevas descripciones de las unidades funcionales. El desempeño alcanzado se muestra en la tabla 6.

4 Conclusiones

Este trabajo muestra un análisis para seleccionar un enfoque adecuado en la arquitectura de la unidad de procesamiento criptográfico, para aumentar la seguridad en las redes de comunicación al manejar (modificar, agregar, actualizar) diversas implementaciones de estándares criptográficos y con un alto desempeño para descongestionar el tráfico de información en las redes de comunicación, implementando algoritmos con diseños sin etapas de segmentación. La unidad de procesamiento propuesta consta de tres partes principales: una biblioteca de

configuraciones de algoritmos criptográficos que puede ser extendida y modificada, un módulo reconfigurable y una unidad de control.

El desempeño de la implementación del algoritmo DES es de 917 Mbps. El diseño consta de cuatro rondas completamente desenrolladas que utiliza demasiados recursos del FPGA para el ruteo, aumentando el tiempo del camino crítico y reduciendo el desempeño. Trabajo a futuro es tener una implementación que use la memoria empotrada del dispositivo para reducir la lógica de ruteo, disminuir el tiempo del camino crítico y aumentar el desempeño.

Las implementaciones a 1Gbps de los algoritmos AES, SHA-1 y MD5, donde SHA-1 y MD5 son las soluciones en FPGA con el mayor desempeño las cuales son reportadas en [14] y [15], respectivamente.

Referencias

1. Orlando, G.: Efficient Elliptic Curve Processor Architectures for Field Programmable Logic, Tesis, Worcester Polytechnic Institute (2002)
2. Mel, H.X., Baker, D.: Cryptography Decrypted, Addison-Wesley, EUA (2001)
3. Schneier, B.:Applied Cryptography: Protocols, Algorithms and Source Code in C, John Wiley and Sons, EUA (1996)
4. Compton, K., Hauck, S.: Reconfigurable Computing: A Survey of Systems and Software In: ACM Computing Surveys Vol. 34 No. 2, (2002)
5. Wu L., Weaver C., Austin T.: CryptoManiac: A Fast Flexible Architecture for Secure Communication, ACM/IEEE 28th International Symposium on Computer Architecture (ISCA-2001)
6. Buchty R.: Cryptonite – A Programmable Crypto Processor Architecture For High-Bandwidth Applications, Tesis, Technischen Universitat Munchen, (2002)
7. Taylor, R.R., Goldstein, S.C.: A High-Performance Flexible Architecture for Cryptography, In Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems 1999.
8. Elbirt, A.J.: Reconfigurable Computing for Symmetric Algorithms, Tesis, Worcester Polytechnic Institute, (2002)
9. Federal Information Processing Standards (FIPS) Publication 46-3.: Data Encryption Standard (DES), US DoC/NIST, (1999)
10. Federal Information Processing Standards (FIPS) Publication 197.: Announcing the Advanced Encryption Standard (AES), US DoC/NIST, (2001)
11. Federal Information Processing Standards (FIPS) Publication 180.: Announcing the Secure Hash Standard, US DoC/NIST, (2002)
12. Rivest, R.: The MD5 Message-Digest Algorithm, RFC 1321, MIT and RSA Data Security, Inc., (1992)
13. Algredo-Badillo, I., Cumplido-Parra R. A., Feregrino-Uribe C.: Implementación de un Módulo SHA-1 para una Plataforma Reconfigurable Criptográfica en FPGA a 1 Gbps. Por aparecer en International Conference on Reconfigurable Computing and FPGAs, ReConFig04, México (2004)
14. Algredo-Badillo, I., Cumplido-Parra R. A., Feregrino-Uribe C.: Desarrollo de un Módulo MD5 para un Sistema Criptográfico Reconfigurable en un FPGA. Por aparecer en International Conference on Reconfigurable Computing and FPGAs, ReConFig04, México (2004)