IMPLEMENTACION DE AES EN FPGA

Javier Fernando Castaño¹, Fabián Velásquez Clavijo¹

¹Grupo de Investigación Macrypt
Escuela de Ingeniería
Universidad de los Llanos - Colombia
[jfcastano, fvelasquez]@unillanos.edu.co

This paper presents the design and implementation of hardware architecture of AES-Rijndael, using an FPGA reconfigurable logic device Xilinx XC3S500E on a development board Digilent Spartan 3E Starter. This implementation performs encryption and decryption of data blocks and supports 128-bit key. 4 parallel multipliers are implemented in the finite field $GF(2^8)$ to optimize the process of decryption. It implements an iterative architecture in which a round of the Rijndael algorithm is done completely in parallel, greatly increasing the performance of the processes of encryption and decryption. It also implements the subkey generation concurrently.

INTRODUCCION

La seguridad informática ha adquirido gran importancia en las áreas de la industria, los negocios y en la sociedad actual. Las técnicas básicas que se requieren para proteger la información corresponden al campo de la criptografía, debido a que ésta es aplicada a la seguridad y es una herramienta primordial para asegurar confidencialidad en la transmisión y almacenamiento de la información.

AES es el actual estándar de cifrado simétrico dispuesto por el NIST (National Institute of Standards and Technology), después de un periodo de prueba entre quince algoritmos sometidos, a través de la cual en el 2000 fue designado el algoritmo Rijndael como AES (Angel 2002); el Standard reemplazó el T-DES.

El algoritmo Rijndael opera a nivel de bytes, interpretando estos como elementos de un campo de Galois $GF(2^8)$, y a nivel de registros de 32 bits, considerándolos como polinomios de grado menor que 4 con coeficientes que son a su vez son polinomios en $GF(2^8)$, como se plantea en Daemen (2001) y se estandariza en NIST (2001).

En este trabajo se implementó la arquitectura hardware para el algoritmo Rijndael-AES en una FPGA, desarrollando el proceso de cifrado y descifrado, ejecutando una evaluación de las ventajas que tiene el algoritmo Rijndael con relación a su seguridad y optimización.

ESTADO DEL ARTE

Los trabajos realizados sobre arquitecturas algorítmicas criptográficas implementadas en campos programables, específicamente en FPGAs

(Field Programmable Gate Array) aumentan día a día.

En Colombia se ha reportado un trabajo realizado en la Universidad del Valle [46]. Otras investigaciones que se han realizado de AES son Bertoni (2002), López (2006), López (2003), Liberatori (2004), Nazar (2003), entre otras.

RESULTADOS

Los resultados se presentan en la Tabla 1, comparando con implementaciones realizadas en otros trabajos.

Tabla 1: Comparación con otras Implementaciones

Autor	Cifrado		Descifrado	
	Throughput Mbps	CLs	Throughput	CLs
Liberatori (2004)	637.24	1584	500.28	2506
Standaert et al.[33]	1450	542	No implementa	NI
Segredo et al. (2004)	417	496	NI	NI
Lopez (2003)	6.8	2500	4.5	2400
López (2005)	1067.62	633		
Este trabajo	660	410	660	840

ANÁLISIS DE RESULTADOS

Es posible considerar algunos factores que influyen en los resultados obtenidos.

Existen ventajas inherentes a los dispositivos FPGA, dada su arquitectura paralela y la posibilidad de procesamiento concurrente. Este hecho se evidenció en la implementación del prototipo, en el cual predominan los bloques paralelos y las conexiones masivas de elementos en cascada, logrando flujo de datos sin retardos significativos.

De igual manera, se debe tener en cuenta la optimización lograda en el bloque KeySch, el cual se implementó completamente en paralelo, logrando la generación de la subclave directamente y sin retardos.

Otro punto importante de optimización, es el uso de multiplicadores paralelos en la transformación mixcolumns del descifrado, logrando también reducir el área ocupada por dicho bloque.

CONCLUSIONES

En el presente trabajo se obtuvieron resultados importantes implementando la arquitectura iterativa del algoritmo AES-Rijndael. En este caso se pudo notar las ventajas de trabajar en hardware, sobre todo aprovechando las características de los dispositivos FPGA.

Si se compara el throughput y el desempeño en general de las aplicaciones en software y hardware reportadas, es evidente la superioridad de estas últimas, permitiendo una mayor tasa de transferencia de información para los procesos de cifrado y descifrado.

La mayor parte de la optimización resultante en las aplicaciones hardware se deben al uso de paralelismo, como en el caso de la transformación subbytes, que se realiza sin ningún tipo de retardo, mientras que en una aplicación software se requieren 16 operaciones secuenciales.

Se lograron optimizaciones adicionales, principalmente por una comprensión de la naturaleza estructural de ciertos módulos, como en el caso del proceso de key schedule (generación de subclaves); esta mejor implementación redundó en una reducción de los recursos usados en la FPGA (área ocupada).

La experiencia adquirida en el desarrollo del presente trabajo es muy valiosa, logrando un dominio del funcionamiento del algoritmo en

forma total, además un conocimiento en VHDL alto, enriqueciendo de esta manera el quehacer académico de la Universidad de los Llanos, en donde el Grupo Macrypt está usando este desarrollo en varios proyectos de investigación.

REFERENCIAS

- Angel, J. (2005) "AES -Advanced Encryption Standard". CINVESTAV México.
- Bertoni, G. y Racchetti, M. (2002), "Hardware implementation of the rijndael s-box: a case study", Alari, Università della Svizzera Italiana Politecnico di Milano.
- Daemen, J. y Rijmen, V. (2001). "AES Proposal: Rijndael".
- Liberatori, M. (2004) "Desarrollo de Encriptado AES en FPGA", Maestría en Redes de Datos, Universidad de la Plata.
- López, E. (2005), "Implementación Eficiente en FPGA del Modo CCM usando AES", Maestría en Ciencias del Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional, México.
- López, J. et. al. (2003) "Implementación en Hardware del Algoritmo Rijndael" Grupo de Bioelectrónica y Nanoelectrónica, Escuela IEEE, Universidad del Valle.
- Nazar, S. (2003) "AES Algorithm Implementation - An devised for efficient implementations on reconfigurable devices". IEEE Computer Society Press.
- NIST (2001) Announcing the ADVANCED ENCRYPTION STANDARD (AES). Federal Information Standards Publication.
- Standaert, F. (2003) "Efficient Implementation of Rijndael Encryption in Reconfigurable Hardware: Improvements and Design Tradeoffs". *Cryptographic Hardware and Embedded Systems-CHES 2003, pages 334-350, 2003.*
- Segredo, A. et. al. (2004). Diseño de un procesador criptográfico Rijndael en FPGA. *X Workshop IBERCHIP, pag. 64*