Universidad de Costa Rica
Facultad de Ingeniería
Escuela de Ingeniería Eléctrica

Implementación y análisis de algoritmos de encriptación en un FPGA.

Por:

Alejandro León Torres

Ciudad Universitaria "Rodrigo Facio", Costa Rica

Noviembre de 2015

Implementación y análisis de algoritmos de encriptación en un FPGA.

Por:

Alejandro León Torres

IE-0499 Proyecto eléctrico

Aprobado por el Tribunal:

M.Sc. Diego Valverde Garro
Profesor guía

M.Sc. Carlos Duarte Martínez
Profesor lector

M.Sc. Enrique Coen Alfaro
Profesor lector

Dedicatoria

Dedico este proyecto a las siguientes personas:

- asdas

Reconocimientos

asdasd

Resumen

El proyecto busca investigar sobre la teoría de criptografía y como la misma es implementada en la computación para el resguardo de datos, específicamente en hardware haciendo uso de FPGAs y el lenguaje de descripción de hardware Verilog.

Como punto de partida se elegirán dos algoritmos de encriptación comúnmente empleados, para llevar a cabo un análisis comparativo de una serie de parámetros que son relevantes para su implementación en una plataforma de FPGA. Estos parámetros consideran tres de las mayores limitantes para implementación de algoritmos en FPGA, como son el consumo de celdas, la cantidad de memoria interna utilizada y finalmente el uso de celdas especializadas de aritmética o DSP.

Índice general

Índice de figuras

Índice de tablas

1 Introducción

1.1 Justificación

La encriptación de datos por seguridad es una necesidad en la actualidad. Por ejemplo cuando a un empleado le roban una computadora corporativa que contiene datos sensibles para la empresa en la que labora, la encriptación evita que se pueda acceder a los mismos y que así se protejan de terceros.

En el caso de la encriptación de software trae consigo problemáticas como lo son la necesidad de actualizaciones y el desempeño del computador. Este último aspecto se debe a que una encriptación a nivel de software debe dedicar recursos del sistema a encriptar/desencriptar información.

En el caso de hardware se tienen los beneficios de que es muy confiable, rápido y conveniente. A diferencia de la encriptación de software se tiene una parte de hardware dedicada al proceso de encriptación/descriptación y por tanto el desempeño de la computadora no se ve tan afectado, también al no haber forma de actualizar hardware ocurre una disminución en costos (ACA FALTA LA CITA). Otra de las grandes ventajas de la encriptación basada en hardware es la facilidad de configuración, ya que gran parte de esto proceso es eliminado debido a que el hardware se encarga directamente de esto. (CITA DE DRIVETRUST).

Debido a lo expuesto anteriormente se buscó trabajar en algoritmos de encriptación en hardware ya que es un área de trabajo que se puede explotar para investigar y mejorar.

Se escogió como plataforma de trabajo un FPGA

1.2 Alcances y limitaciones del proyecto

Se implementarán 2 algoritmos de encriptación de datos en un FPGA haciendo uso de Verilog como lenguaje de descripción de hardware.

Posteriomente y mediante las herramientas de síntesis de Xilinx se realizará un análisis de métricas críticas en el desarrollo de aplicaciones en FPGAs como los son la cantidad de compuertas o celdas, el consumo de memoria interna del FPGA así como la cantidad de bloques aritméticos o de DSP que son usados por cada algoritmo.

Inicialmente se va a llevar a cabo un análisis individual de cada algoritmo, haciendo uso de las métricas anteriormente descritas y variando parámetros

comunes de los algoritmos de encriptación como lo son el tamaño de la llave y la cantidad de rondas de encriptación (este último en algoritmos de tipo Feistel).

Como segunda parte del proyecto se va a realizar un análisis comparativo entre ambos algoritmos eligiendo parámetros fijos para ambos.

Los análisis individuales y comparativos anteriomente mencionados no abarcarán ningún tipo de criptoanálisis de algún algoritmo con respecto otro ni de cuál sería la escogencia de los parámetros ideal para realizar un análisis comparativo entre ambos. Sino que a partir del análisis individual realizado se va a efectuar una escogencia de los parámetros de ambos algoritmos para realizar su comparación implementando las métricas descritas.

Para la escogencia de estos dos algoritmos se realizará a partir de una identificación de las principales ramas del cifrado para así elegir los dos algoritmos de dos de estas ramas abarcando de esta manera un tema más amplio para el análisis y discusión.

Se limitará a realizar una escogencia de esta manera sin la necesidad de realizar un criptoanálisis de los algoritmos, y más bien se simplificará a buscar algoritmos que sean implementables, de manera relativamente sencilla, en un FPGA conociendo desde un principio las limitantes estáticas del hardware.

1.3 Objetivos

Objetivo General

Implementar dos algoritmos de encriptación en un FPGA y realizar un análisis comparativo de la implementación de ambos algoritmos, empleando una serie de parámetros previamente seleccionados.

Objetivos Específicos

1. Implementar dos algoritmos de encriptación comúnmente empleados en un FPGA utilizando el lenguaje de descripción de hardware Verilog.

2. Realizar un análisis individual para cada uno de los algoritmos individuales, variando alguno de sus parámetros (por ejemplo el tamaño de la llave) para comparar haciendo uso de métricas como la cantidad de compuertas, el consumo de memoria interna del FPGA así como la cantidad de bloques aritméticos o de DSP que se van a ir utilizando conforme se varíe el parámetro del algoritmo elegido.

3. Realizar un análisis comparativo de los dos algoritmos implementados, utilizando como métricas la cantidad de compuertas o celdas, el con-

sumo de memoria interna del FPGA así como la cantidad de bloques aritméticos o de DSP que son usados por cada algoritmo.

1.4 Metodología

La metodología que se siguió para la realización del proyecto es la siguiente:

1. Estudios bibliográficos de:
   - Criptografía: importancia y como la misma se implementa en la computación.
   - Algoritmos de cifrado: Identificación de ramas y subramas.
   - Código e implementación de algoritmos de encriptación en diferentes lenguajes de programación.
2. Escogencia de los algoritmos de encriptación a implementar.
3. Implementación de los algoritmos de cifrado en un FPGA Xilinx MODELO????.
4. Realización del análisis individual de cada uno de los algoritmos.
5. Realización del análisis comparativo entre ambos algoritmos.
6. Realización de las conclusiones y Recomendaciones.

1.5 Desarrollo

El presente informe se estructura para el lector de la siguiente manera:

1. Capítulo I: Introducción.
2. Capítulo II: Antecedentes y Marco Teórico.
3. Capítulo III: Implementación de los algoritmos de encriptación en el FPGA.
4. Capítulo IV: Resultados de los análisis individuales y comparativos de los 2 algoritmos implementados en el FPGA.
5. Capítulo V: Conclusiones y recomendaciones.

2 Marco Teórico

Este capítulo va a poner en contexto al lector con respecto a conceptos básicos de criptografía para posteriormente explicar los algoritmos que van a ser implementados en el FPGA.[1]

Conceptos Básicos

Según la Real Academia Española **?** la criptografía se define como

Arte de escribir con clave secreta o de un modo enigmático.

El mensaje que se desea transmitir es usualmente llamado *texto plano* o simplemente *mensaje*. Este mensaje pasa por un proceso donde se disfraza el texto plano en un *texto cifrado*, el proceso es llamado *cifrado*. El proceso inverso donde se toma un texto cifrado en un texto plano se denomina *descifrado*.

El texto plano o mensaje se denota usualmente por la letra M o P, el texto cifrado se denota usualmente por la letra C, la función o algoritmo que cifra se denota por E y la que descrifa se denota por D. Un algoritmo criptográfico corresponde a la función matemática para cifrar y descrifrar.
Se muestra en las Ecuaciones 2.1 y 2.2 las relaciones entre estas notaciones. Note como al aplicarle la función de cifrado al texto plano se obtiene el texto cifrado y como al aplicarle la función de descifrado al texto cifrado se obtiene el texto plano. Finalmente se debe cumplir la identidad que describe la Ecuación 2.3. **?**

$$E(M) = C \tag{2.1}$$

$$D(C) = M \tag{2.2}$$

$$D(E(M)) = M \tag{2.3}$$

La importancia de criptografía transciende más allá de brindar la confidencialidad en la comunicación la criptografía también cumple con la siguientes tareas:

- Autenticación: El receptor del mensaje debe de poder conocer y asegurar el emisor del mensaje, esto para que un tercero no pueda adjudicarse la identidad del emisor.

[1] Según el ISO 7498-2 los términos correctos para encriptar y desencriptar son cifrar y descifrar respectivamente.

- Integridad: El receptor tiene que poder asegurarse que el mensaje no fue cambiado en el transito del mismo. Esto para que un tercero no pueda cambiar el contenido enviado por el emisor sin que el receptor lo sepa.

- *Non-repudiation*: El emisor del mensaje no puede negar que el mensaje fue enviado por él.

Sistema criptográfico *criptosistema*

Cuando la seguridad del algoritmo se basa en como procede el algoritmo, se denomina *algoritmo restringido*. Este tipo de algoritmos son poco utilizados en la actualidad debido al gran problema que presentan. Tomemos de ejemplo que un grupo de usuarios decide utilizar un algoritmo de cifrado restringido para sus comunicaciones, se tendrá una comunicación segura hasta que alguno de los miembros decida salirse del grupo, ya que el usuario al no pertenecer más al grupo, no le importa mantener en secreto el algoritmo y puede distribuirlo para que terceros intercepen las comunicaciones de ese grupo. Así cada vez que un miembro deja el grupo, el grupo debe proceder a cambiarse a todo un nuevo algoritmo lo cual puede tornarse una labor complicada.

En cambio la criptografía moderna agrega el concepto de *llave* donde se tiene un algoritmo el cual toma como parámetro de entrada una llave y el texto plano o texto cifrado y cifra o descifra el mismo de forma correcta únicamente si se tiene la llave correcta. Así volviendo al ejemplo anterior, el grupo solamente necesitaría cambiar de llave cuando un miembro se va, facilitando el uso del cifrado y manteniendo las comunicaciones secretas.

Este concepto anterior viene a definir lo que actualmente se conoce como sistema criptográfico o *criptosistema*. Según **?** un criptosistema cuenta con 5 componentes:

- Un espacio de textos planos o mensajes (M)

- Un espacio de textos cifrados (C)

- Un espacio de llaves (k)

- Una familia de *transformaciones de cifrado*: $E_K : M \to C$ donde $K \epsilon k$

- Una familia de *transformaciones de descrifrado*: $C_K : C \to M$ donde $K \epsilon k$

Se entiende como *espacio* el conjunto de posibles valores para la variable dada, sea esta M, C o K. Y una familia de transformaciones son todos los posibles mapeos que se pueden realizar de un espacio a otro (de M a C o viceversa) con todos los valores contenidos en el espacio k.

En la actualidad se trabaja la criptografía sobre computadoras, es decir, cifrando y descrifrando bits, los cuales pueden tener diferentes significados, ya sea una imagen, un texto, un programa, etc. Esto significa que en la actualidad no se trabaja sobre caracteres del alfabeto o símbolos, sino más bien sobre 1's y 0's. Esto toma relevancia ya que al tener solo dos símbolos para cifrar, los algoritmos se vuelven más complejos por la falta de alternativas para sustituir un símbolo por otro.

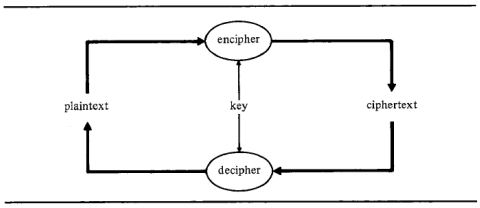

Figura 2.1: Descripción gráfica de un sistema criptográfico.