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

Software solutions for hard drives have been available for some time now. They have often been criticized for being inconvenient, slow and like any other software, prone to needing updates.

In contrast, hardware encryption is very reliable, fast and convenient. Hardware encryption doesn't require system resources to perform the encryption/decryption process and therefore allows for better system performance. Since hardware encrypted drives are not subject to updates, the costs related to traditional software solutions are eliminated. Another great advantage of hardware encrypted drives, they can be easily reset. This reduces the amount of time spent scrubbing the drive or erasing disk data, which in turn stretches the IT department budgets when redeployment of assets is necessary.

Data encryption is no longer a luxury. It's a necessity. Organizations and users with sensitive data in use on laptops and desktops have no choice but to secure data on disk drives in a manner that is reasonable to regulators.

Software-based encryption products address the basic need for encrypting data on computer systems where performance is not the primary concern or where disk encryption is a part of a larger set of data privacy requirements. Examples of this include communications and messaging encryption requirements. Software-based products can also provide encryption at the file and folder level, as well as for removable storage devices.

Hardware-based encryption overcomes the two most significant barriers to widespread adoption of encryption technology — ease of use and system performance. Encryption built into the hard disk eliminates much of the setup and configuration complexity. DriveTrust isolates the encryption functions and stores the encryption keys in the hard drive itself, providing an added security benefit of blocking rootkits and other malware from accessing keys and other sensitive information from the operating system. In addition, hardware encryption performance is very close to that of a non-encrypted drive with minimal impact on computing operations, far superior to software-based encryption. Hardware-based encryption is well-suited to mobile user populations where performance and ease of implementation and use are concerns

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 consumo 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.