

### UNIVERSIDAD NACIONAL DE CÓRDOBA

### FCEFyN

### ANTEPROYECTO DEL PROYECTO INTEGRADOR DE INGENIERÍA EN COMPUTACIÓN

### DISEÑO E IMPLEMENTACIÓN DE

### AES-GCM PARA REDES ÓPTICAS

Autor: BARBIANI, GIANFRANCO

Mat.: 36.372.639

Director: Dr. Mario Hueda CoDirector: Dr. Damián Morero

### Diseño e Implementación de AES-GCM para Redes Ópticas

### 1. Introducción

En el día de hoy comunicarse a través de medios digitales de diversa índole resulta natural, ya sea entre particulares o entre entidades más grandes. Es por ello que el contenido de los mensajes que componen dicha comunicación puede poseer diferentes tópicos y existen, pues, casos en que este mensaje posee una importancia tal, que no debe ser conocido por nadie más que el emisor y receptor. Debido a eso, el medio por el que se estableció la comunicación debe proveer algún tipo de protección contra agentes externos. Los medios digitales actuales necesitan establecer entonces, enlaces baratos y rápidos, pero también confiables, para evitar que un tercero vea, o modifique el mensaje. Con ese objetivo, la industria de las telecomunicaciones por fibra óptica está comenzando a integrar sistemas que aseguren la confidencialidad y la autenticidad del mensaje efectivamente, pero que también puedan trabajar con los grandes volúmenes de datos y a la alta velocidad con la que esta tecnología se maneja.

Dentro del marco de seguridad aparecen diferentes estándares que introducen algoritmos criptográficos que proveen protección de los mensajes. Existe particularmente una institución que es pionera en la publicación de documentos que describen estos estándares, llamada “National Institute of Standards and Technology” (NIST). Uno de dichos documentos, “Federal Information Processing Standards Publications 197” (FIPS PUB 197), especifica el algoritmo criptográfico “Advanced Encryption Standard” (AES) usado para proteger datos electrónicos.

AES presenta un nivel de protección tal que:

* La “National Security Agency” (NSA) de los Estados Unidos lo utiliza para cifrar datos clasificados como “TOP SECRET”.
* Tiene un solo ataque exitoso registrado en el 2011, llevado a cabo por un grupo de investigadores de Microsoft y de la Dutch Katholieke Universiteit Leuven.
* No es vulnerable al criptoanálisis diferencial y lineal.
* Es necesaria una gran cantidad de textos encriptados y gran procesamiento para su análisis.
* Para poder romper AES serían necesarios un billón de ordenadores, que cada uno pueda probar mil millones de claves por segundo y unos 2000 millones de años para dar con un AES con clave de 128 bits (existe AES-256).

A pesar de que AES provee una confidencialidad remarcable, existe un parámetro de seguridad que pasa por alto y que los sistemas informáticos deben también garantizar, la *integridad*, la cual está ligada a la autenticidad del mensaje. Para suprimir esta carencia, AES pasa a formar parte de un algoritmo mayor, denominado “Galois/Counter Mode” (GCM). GCM es un modo de operación de los algoritmos de cifrado por bloques, y se encuentra especificado en la “Special Publication 800-38D” del NIST y algunas de sus características son:

* GCM es construido a partir de un cifrado por bloque con clave simétrica de 128/192/526 bits, como AES.
* Es un modo de operación del algoritmo AES.
* Provee confidencialidad de datos, usando una variante de “Counter” (modo de operación CTR) para encriptar.
* Provee autenticidad de los datos confidenciales (hasta 64 GB por invocación) usando una función universal Hash que es definida sobre una campo de Galois binario.
* Puede también proveer autenticación para datos adicionales (de largo prácticamente ilimitado por invocación) que no son encriptados.
* Si el input es solo datos que no van a ser encriptados, entonces GCM se llama GMAC; que es simplemente un modo de autenticación sobre la input data.
* Provee una autenticación más fuerte que un checksum (no criptográfico) o un código de detección de errores. En particular, GCM puede detectar ambos:
  + Modificaciones accidentales de datos y
  + Modificaciones intencionales no autorizadas.

Tanto AES como GCM fueron diseñados para poder ser implementados en Software y en Hardware, esta última de importante interés ya que puede aprovechar el paralelismo de la electrónica para efectuar la gran mayoría de las operaciones de dichos algoritmos, logrando un alto throughput (bits/frecuencia), bajo costo y baja latencia.

### 2. Objetivos Generales

El objetivo general del presente Proyecto Integrador es recorrer el flujo de desarrollo de los algoritmos AES y GCM para aplicaciones en redes ópticas. Para esto, se propone realizar el diseño, desarrollo, simulación y emulación de un código que se desempeñe cumpliendo las normas estipuladas por el FIPS 197 y SP 800-38D. Se prestará especial atención al diseño de la arquitectura de manera de aumentar el paralelismo y así incrementar el rendimiento; contemplando también reducir el conexionado de los bloques constituyentes, el cual tiene un importante impacto en la complejidad de implementación. Además, para la verificación experimental del código diseñado, se realizará el desarrollo de una arquitectura para implementar en una FPGA Kintex-7. Esta arquitectura deberá ser parametrizable para poder escalar en el futuro a versiones con diferentes longitudes de bloques y claves.

### 3. Objetivos Particulares

A continuación se listan algunos de los objetivos particulares del presente proyecto:

* Investigar posibles diseños de los algoritmos de AES y GCM a partir de la literatura existente.
* Generar algoritmos de construcción de los diferentes códigos.
* Simular y evaluar el desempeño de diferentes códigos para encontrar la arquitectura que provea el mejor compromiso entre performance y complejidad.
* Desarrollar un simulador en lenguaje C++ para probar los diferentes diseños de códigos en primera instancia.
* Diseñar la arquitectura de implementación del código.
* Adaptar el simulador escrito en lenguaje C++ a la arquitectura propuesta del código con variables en punto fijo.
* Escribir la arquitectura de implementación en el lenguaje de descripción de Hardware Verilog.
* Desarrollar un banco de pruebas parametrizable para verificar la implementación del código.

### 4. Metodología de trabajo

La metodología de trabajo del presente proyecto consiste de dos etapas principales: *diseño del código* y la *implementación* del mismo en una FPGA.

Para la realización de la primer etapa, en principio se buscará bibliografía acerca de Advanced Encryption Standard (AES), del modo de operación de cifrado en bloque Counter (CTR) y del modo de operación de cifrado en bloque *autenticado* Galois/Counter Mode (GCM) y se investigará si puede cumplir con los requisitos que la comunicación por fibra óptica exige. Una vez que se cuente con una base firme de los códigos a desarrollar, y sus alcances y limitaciones, se procederá al desarrollo en Software del simulador en lenguaje C++ para medir el rendimiento de los algoritmos, comparándolo con resultados teóricos esperados. Posteriormente se procederá a investigar profundamente la mejor manera de paralelizar los algoritmos para sacar el mayor provecho del Hardware disponible.

En la segunda etapa del trabajo se diseñará e implementará la arquitectura de AES-GCM en una FPGA con el fin de medir el rendimiento y la complejidad. Para llevar esto a cabo se deberá crear un banco de pruebas que permita controlar los parámetros de emulación. Este banco de pruebas deberá comunicarse con la PC para la extracción de datos y la configuración de la FPGA. Este diseño de arquitectura deberá contemplar la utilización óptima de los recursos de la FPGA y la tasa máxima de procesamiento de datos a la que se desea llegar, que es de 1Gbps. Se verificará el funcionamiento de este diseño propuesto con la implementación de un simulador en punto fijo diseñado con la librería de SystemC para el lenguaje C++.

### 5. Herramientas de trabajo

A continuación se muestran los recursos que se disponen para la realización del proyecto:

* Entorno de trabajo para los lenguajes C/C++.
* Acceso a papers y libros donde se desarrolle el tema.
* Herramientas para Simulación del lenguaje Verilog (Xilinx Vivado).
* Kit de desarrollo KC-705 de Xilinx, el cual posee una FPGA Kintex-7 en su interior.
* Herramienta de desarrollo del software para el microprocesador a implementar en la FPGA (Xilinx SDK).
* Librería “SystemC” para la simulación de variables en punto fijo.

### 6. Motivación e importancia del proyecto

* La incursión en el estudio de algoritmos criptográficos de vanguardia.
* La posibilidad de atravesar todo el flujo de diseño de un chip VLSI.
* La posibilidad de contribuir al avance de los sistemas de comunicaciones.
* La aplicación de conocimientos adquiridos a lo largo de la carrera de Ingeniería en Computación en un producto que puede llegar al mercado.
* La posibilidad de realizar publicaciones científicas acerca de lo desarrollado en el proyecto.

### 7. Cronograma

Se establecerá un cronograma con las etapas de trabajo y la fecha planificada de finalización de las mismas.

|  |  |  |  |
| --- | --- | --- | --- |
| **Fecha Inicio** | **Duración** | **Fecha Finalización** | **Etapa** |
| 27/05/2016 | 2 semanas | 08/07/2016 | Desarrollo de simulador AES en “C++” |
| 11/07/2016 | 2 semanas | 22/07/2019 | Desarrollo de simulador GCM en “C++” |
| 25/07/2016 | 1 mes | 26/08/2019 | Diseño de los algoritmos en HW |
| 29/08/2016 | 3 meses | 30/09/2016 | Implementación del banco de pruebas |
| 03/10/2016 | 2 semanas | 14/10/2016 | Desarrollo de simulador en “punto fijo” |
| 17/10/2016 | 3 meses | 13/01/2017 | Diseño e implementación de Arquitectura de los algoritmos |
| 16/01/2017 | 1 mes | 17/02/2017 | Emulación y análisis de resultados |
| 20/02/2017 | 2 meses | 21/04/2017 | Escritura del proyecto integrador |

### 8. Datos del Alumno, Director y Co-Director

**Nombre Alumno**: Barbiani Gianfranco

**Carrera**: Ingeniería en Computación

**Teléfono**: 0351-152093135

**E-mail**: Gianfranco.barbiani@gmail.com

**Director**: Dr. Mario Hueda

**Cargo**: Prof. Titular Teoría de Señales y Sistemas Lineales, Dpto de Electrónica

**E-mail**: mhueda@gmail.com

**CoDirector**: Dr. Damián Morero

**Cargo**: Profesor Asistente de Informática, Departamento de Computación

**E-mail**: dmorero@gmail.com

### 9. Anexo 1:

Aplicaciones estandarizadas de GCM:

|  |  |  |
| --- | --- | --- |
| **Año** | **Estándar** | **Aplicación /Documento** |
| 2004 | ANSI (INCITS) Fibre Chanel Secury Protocols (FC-SP) | Proteger datos a través de fibra óptica.  Doc.: FC-SP ANSI INCITS 1570-D. |
| 2005 | NSA Suite B Cryptography | Programa de Modernizacion Criptográfica.  Doc.: Depertamento de Defecnza de EEUU. |
| 2005 | IETF IPsec Standards | Seguridad en Protocolos de Internet  Doc.: The Use of Galois/Counter Mode (GCM)  in IPsec Encapsulating Security Payload (ESP) |
| 2006 | IEEE 802.1AE (MACsec) Ethernet Security | Seguridad MAC para Entidades (SecY).  Doc.: IEEE 802.1AE. |
| 2007 | IEEE P1619 Standard Architecture for Encrypted Shared Storage Media | Protección de datos alamcenado y su correspondiente clave criptográfica..  Doc.: IEEE P1619/D16. |
| 2007 | IEEE 802.11ad (WiGig) | Redes de área local y metropolitana.  Doc.: IEEE P802.11ad. |
| 2008 | TLS 1.2 (WiFi) | Redes inalámbricas de área local y metropolitana.  Doc.: he Transport Layer Security (TLS) Protocol Version 1.2. |
| 2009 | SSH | Seguridad en Protocolos para Redes.  Doc.: AES Galois Counter Mode for the Secure Shell Transport Layer Protocol. |

### 10. Referencias:

1. Cryptography and Network Security: Principles and Practice.- Quinta Edición.- William Stallings.
2. FIPS 197: “ADVANCED ENCRYPTION STANDARD (AES)”.- Pub. 2001.- National Institute of Standards (NIST).
3. NIST Special Publication 800-38A: “Recommendation for Block Cipher Modes of Operation: Methods and Techniques”.- Edición 2001.- National Institute of Standards (NIST).
4. NIST Special Publication 800-38D: “Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC”.- Pub. 2007.- National Institute of Standards (NIST).