

### UNIVERSIDAD NACIONAL DE CÓRDOBA

### FCEFyN

### ANTEPROYECTO DEL PROYECTO INTEGRADOR DE INGENIERÍA EN COMPUTACIÓN

### DISEÑO E IMPLEMENTACIÓN DEL ALGORITMO GCM-AES EN CIRCUITOS INTEGRADOS PARA REDES ÓPTICAS

Autor: BARBIANI, GIANFRANCO

Mat.: 36.372.639

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

### Diseño e Implementación del Algoritmo GCM-AES en Circuitos Integrados 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 y en particular la empresa ClariPhy Argentina S.A en donde se llevará a cabo este proyecto, 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 128/192/256 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/segundo), 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 circuitos digitales para redes ópticas. Para esto, se propone realizar el diseño, desarrollo y simulación de un código HDL (Lenguaje de Descripción de Hardware) sintetizable (RTL) 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 optimizar la complejidad de implementación; contemplando reducir el conexionado de los bloques constituyentes, el cual tiene un importante impacto en el área del circuito. Además, para la verificación del código diseñado, se realizará una síntesis del mismo usando librerías estándar de celdas lógicas de tecnología CMOS. 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 arquitecturas de implementación en hardware de los algoritmos de AES y GCM a partir de la literatura existente.
* Diseñar la arquitectura de implementación en hardware en base a la investigación del punto anterior.
* Codificar en Verilog la arquitectura diseñada y estimar su complejidad.
* Desarrollar un entorno de verificación en C++ que permita garantizar que el algoritmo implementado cumple todas las normas de los estándares FIPS 197 y SP 800-38D.

### 4. Metodología de trabajo

La metodología de trabajo del presente proyecto consiste de cuatro etapas principales: *(i) Estudio del algoritmo, (ii) Diseño de la arquitectura de implementación en hardware, (iii) Programación en Verilog de dicha arquitectura, (iv) Análisis de complejidad.*

Para la realización de la primer etapa, 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). En particular, se investigará si el algoritmo estándar puede ser usado en comunicaciones de alta velocidad por fibra óptica. Una vez que se cuente con una base firme de los códigos a desarrollar, y sus alcances y limitaciones, se procederá al desarrollo de la arquitectura.

En la segunda etapa, se procederá a investigar profundamente la mejor manera de implementar los algoritmos para obtener un Hardware que logre la menor cantidad de área y consumo de potencia posible para un throughput deseado de 100Gbps.

En la tercera etapa del trabajo se implementará la arquitectura de GCM-AES en Verilog RTL con el fin de medir el rendimiento y la complejidad. Para llevar esto a cabo se deberá crear un banco de pruebas en C++ que permita controlar los parámetros de simulación del código RTL. Este banco de pruebas deberá generar y proveer vectores para ser utilizados como: (a) señales de estímulo para código RTL, y (b) las salidas esperadas. A su vez deberá ser capaz de permitir su uso tanto para el código RTL como del netlist (descripción de la conectividad de un circuito electrónico) generado post-síntesis.

En la última etapa, se realizará una síntesis del código RTL de la arquitectura propuesta y se comparará la complejidad obtenida con distintas soluciones alternativas.

### 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.
* Para la implementación en CMOS la empresa ClariPhy Argentina S.A proveerá las siguientes herramientas:
  + Herramientas para Simulación del lenguaje Verilog (Cadence Simvision) y Verilog conjunto con C++/SystemC.
  + Librerías de tecnología de celdas estándar de CMOS.
  + Herramientas de síntesis de RTL (Cadence RTL-Compiler).
  + Librería SystemC para la simulación de encriptación y autenticación GCM-AES.

### 6. Motivación e importancia del proyecto

* La incursión en el estudio de algoritmos criptográficos de vanguardia.
* Aprendizaje del flujo de desarrollo de circuitos integrados en la empresa ClariPhy Argentina S.A
  + Capacitación en el flujo de diseño de un bloque componente de un circuito VLSI.
  + La posibilidad de contribuir al avance de los sistemas de comunicaciones actuales.
  + La aplicación directa en la industria 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** |
| 13/02/2017 | 2 semanas | 27/02/2017 | Búsqueda de bibliografía y estudio de algoritmos |
| 27/02/2017 | 4 semanas | 27/03/2017 | Diseño de la arquitectura |
| 27/03/2017 | 7 semanas | 08/06/2017 | Diseño de los algoritmos en HW |
| 08/06/2017 | 3 semanas | 29/06/2017 | Implementación del algoritmo |
| 29/06/2017 | 1 semana | 06/07/2017 | Diseño del banco de pruebas |
| 06/07/2017 | 1 semana | 13/072017 | Implementación del banco de pruebas |
| 13/072017 | 1 semana | 20/07/2017 | Ejecución de pruebas |
| 20/07/2017 | 2 semanas | 04/08/2017 | Síntesis y análisis de resultados |
| 04/08/2017 | 3 semanas | 25/08/2017 | 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. Damián Morero

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

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

**CoDirector**: Dr. Mario Hueda

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

**E-mail**: mhueda@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).