Tesis presentada para el Título de de Grado en Ingeniería en Computación

Diseño e Implementación del Algoritmo GCM-AES en Circuitos Integrados para Redes Ópticas

Gianfranco Barbiani

Julio 2017

Escuela de Computación
Facultad de Ciencias Exactas, Físicas y Naturales
Universidad de Córdoba

This is the Dedication.

Resumen

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 rápidos y de bajo costo, 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.

Contents

List of Figures

List of Tables