XIII Coloquio Nacional de Códigos, Criptografía y Áreas Relacionadas (CNCCAR)

24 – 26 DE ABRIL 2019

CDMX

1 1 1 1 1 1 1 1 1 0 0 0 1 1

PALACIO DE MINERÍA

Presentación

En los últimos tiempos se ha vuelto más imperativo proteger la confidencialidad de la información y garantizar su integridad ante probables modificaciones producidas por diversas razones, así como tener la seguridad de que la información trasmitida por cualquier medio de comunicación no sufra algún deterioro. La Criptografía y la Teoría de Códigos, así como la Seguridad Informática, son herramientas que ayudan a resolver esta problemática.

Con este propósito se busca difundir trabajos y resultados de colegas e intercambiar ideas con personas que hacen uso de resultados y técnicas, además promover de esta manera que las nuevas generaciones de profesionistas en las diversas disciplinas relacionadas con estas áreas, identifiquen oportunidades de desarrollo en su formación y quehacer profesional. Desde su primera versión el coloquio ha contado con una gran aceptación por parte del público, prueba de ello es el número creciente de participantes en el mismo. Además, desde sus orígenes, el Coloquio no ha sido lucrativo y ha sido auspiciado y apoyado por instancias académicas como la propia UAM, la UNAM, el IPN, la Sociedad Matemática Mexicana (SMM), entre otras.

Las versiones anteriores han tenido como sede la UAM-Iztapalapa; Dirección General de Servicios de Cómputo Académico (DGSCA), UNAM; Palacio de Minería; Casa de la Primera Imprenta de América, y la Facultad de Ciencias de la Universidad Autónoma del Estado de México y la Facultad de Ciencias Físico-Matemáticas de la BUAP. En ésta ocasión, el evento se celebra nuevamente en el Palacio de Minería.

En versiones anteriores del coloquio, se ha contado con la participación de investigadores de reconocido prestigio internacional en teoría de códigos, criptografía o campos finitos, entre los que se pueden mencionar a: Neal Koblitz (University of Washington, USA), Alfred J. Menezes (U. de Waterloo, Canada), Iwan Duursma (University of Illinois, Urbana-Champaign, USA), Carlos Moreno (CUNY, Nueva York, USA), Claude Carlet (INRIA, U. Paris, France), Josh Benaloh (Microsoft Research, USA), Daniel Panario (Carleton University, Canada), Levent Ertaul (California State University, USA), Juan Tena, Ignacio Farrán y Edgar Martínez Moro, los tres de la Universidad de Valladolid, España, Robert Morelos-Zaragoza (State University, San Jose, CA, USA), Daniel Cabarcas-Jaramillo de la Facultad de Ciencias de la Universidad de Colombia, Colombia; Rafael H. Villarreal Rodríguez del Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional, México, entre otros. En esta ocasión participan en el coloquio los investigadores Neal Koblitz (University of Washington, USA) e Ivelisse Rubio (Universidad de Puerto Rico, P. Rico)

Este décimo tercer coloquio ha sido posible gracias al apoyo de las siguientes instituciones:

- Universidad Autónoma Metropolitana-Unidad Iztapalapa, a través del Departamento de Matemáticas y la División de Ciencias Básicas e Ingeniería
- Instituto Politécnico Nacional, a través de la Escuela Superior de Ingeniería Mecánica y Eléctrica - Culhuacán, y de la Escuela Superior de Cómputo

- Universidad Nacional Autónoma de México, a través de la Facultad de Ingeniería

Nuestro agradecimiento a los conferencistas e investigadores que comparten sus conocimientos y experiencias en este evento, y a los asistentes por su interés en el mismo. Finalmente, deseamos reconocer el intenso trabajo de todas las personas que han apoyado en los distintos aspectos de la organización del coloquio, y al Palacio de Minería por habernos facilitado sus instalaciones.

Esperamos seguir contando con su apoyo e interés para la realización del 14° Coloquio Nacional de Códigos, Criptografía y Áreas Relacionadas.

¡Hasta pronto!

Abril, 2019

ATENTAMENTE,

EL COMITÉ ORGANIZADOR

Sandra Díaz Santiago
ESCOM, IPN
sdiazsa@ipn.mx

Gina Gallegos García
ESIME, Culhuacán
ggallegosg@ipn.mx

Francisco García Ugalde
Facultad de Ingeniería, UNAM
fgarciau@unam.mx

José Noé Gutiérrez Herrera
Depto. de Matemáticas, UAM-I
ngh@xanum.uam.mx

Horacio Tapia Recillas
Depto. de Matemáticas, UAM-I
htr@xanum.uam.mx

Elaboró: José Noé Gutiérrez Herrera

Horario de actividades

	Miércoles	**Jueves**	**Viernes**
09:00-09:40	Inscripción		
09:40-10:00	1. B. González		
10:00-10:20	2. L.N. Borbolla	11. C.J. Villaseñor	20. F.D. de Melo
10:20-10:40	3. J.A. Bernal	12. E. Camps	21. D. Becerra
10:40-11:00	Inscripción	13. L.R. Nava	22. R. Espinosa
11:00-11:20	Inauguración	Neal Koblitz	Ivelisse Rubio
11:20-11:40			
11:40-12:00	**CAFÉ**		
12:00-12:20	4. J.J. Simón	**CAFÉ**	**CAFÉ**
12:20-12:40	Neal Koblitz	Ivelisse Rubio	
12:40-13:00			23. F.J. González
13:00-13:20			24. B. Ramos
13:20-15:20	**COMIDA**	**COMIDA**	**COMIDA**
15:20-15:40		14. J.J. Angel	25. J. Rodríguez
15:40-16:00	5. P.I. Soto	15. L. Peña	26. E.J. Garcia
16:00-16:20	6. M. García	16. J. Carrillo	27. D. Cervantes
16:20-16:40	7. D. Núñez	**CAFÉ**	**CAFÉ**
16:40-17:00	**CAFÉ**	17. H.S. Pacheco	28. H. Tapia
17:00-17:20	8. J.C. Ku	18. N.A. Ramírez	29. J.J. Gómez
17:20-17:40	9. J. López	19. D. Mata	30. V.G. Reyes
17:40-18:00	10. J.J. Chi		Clausura

Horario de actividades

Miércoles

09:00-09:40 Inscripción
09:40-10:00 1. González Flores Byron. Centro de Investigación en Computación. **Network Scan Detection**

10:00-10:20 2. Laura Natalia Borbolla Palacios. Instituto Politécnico Nacional, ESCOM. **Tokenización 101**

10:20-10:40 3. José A. Bernal. Centro de Investigación y de Estudios Avanzados del IPN. **Multiplicador RNS en VHDL 10:40-11:00** Inscripción

11:00-11:40 Inauguración

11:40-12:00 CAFÉ

12:00-12:20 4. Juan Jacobo Simón Pinero. Universidad de Murcia, Murcia, España. **Conjuntos de información a partir de conjuntos de definición para códigos de Reed-Muller de primer y segundo orden**

12:20-13:20 Neal Koblitz. University of Washington, USA. **La Computación Cuántica y la Criptografía**

13:20-15:40 COMIDA

15:40-16:00 5. Pablo Ignacio Soto Blancas. Universidad Autónoma de la Ciudad de México. **Contrucción de firmas digitales**

16:00-16:20 6. García-Martínez M. Tecnológico de Monterrey, Escuela de Ingeniería y Ciencias, Potosí. **Implementación de la máquina ENIGMA en LABVIEW**

16:20-16:40 7. Diana Nuñez Ramirez. Instituto Politécnico Nacional. Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacán. Sección de Estudios de Posgrado e Investigación. **Marca de agua híbrida para aumentar la seguridad en ultrasonidos médicos digitales**

16:40-17:00 CAFÉ

17:00-17:20 8. Juan Carlos Ku Cauich. Departamento de Computación, Centro de Investigación y de Estudios Avanzados del IPN. **Polinomios básicos primitivos y representaciones de elementos en un anillo de Galois**

17:20-17:40 9. Joel López Romero. Instituto Politénico Nacional - ESCOM. **Diseño en hardware de un cifrador ligero**

17:40-18:00 10. Jesús Javier Chi Domínguez. Cinvestav IPN, Departamento de computación. **De la búsqueda de raíces polinómicas**

Jueves

10:00-10:20 11. Carolina Jeanette Villaseñor Rodelas. Universidad Nacional Autónoma de México, FES Cuautitlán. **Criptoanálisis físico contra dispositivos electrónicos embebidos, y su protección**

10:20-10:40 12. Eduardo Camps Moreno. ESFM-IPN. **Códigos polares sobre Curvas Castillo**

10:40-11:00 13. Luis Roberto Nava Lara. Escuela Superior de Cómputo - IPN. **Generación de S-Boxes usando la ecuación logística**

11:00-12:00 Neal Koblitz. University of Washington, USA. **Las Criptomonedas**

12:00-12:20 CAFÉ

12:20-13:20 Ivelisse Rubio. Departamento de Ciencia de Cómputos, Universidad de Puerto Rico, Río Piedras. **Análisis de la complejidad lineal de arreglos multidimensionales periódicos**

13:20-15:20 COMIDA

15:20-15:40 14. José de Jesús Angel Angel. Universidad Anáhuac, Huixquilucan, Estado de México. **BlockChains y sus aplicaciones**

15:40-16:00 15. Leticia Peña Téllez. Facultad de Ciencias UAEMéx. **Cifrado basado en álgebras de conglomerado**

16:00-16:20 16. Dr. Jesús Carrillo Pacheco. Academia de Matemáticas, Universidad Autónoma de la Ciudad de México. **Matrices L-G y Teoría de Códigos**

16:20-16:40 CAFÉ

16:40-17:00 17. Hugo Sebastian Pacheco Rodríguez. Centro de Investigacíon en Computaciíon. **Neural Networks Applied to Network Scan Detection**

17:00-17:20 18. Néstor Alejandro Ramírez García. Instituto Politécnico Nacional, ESCOM. **Transmisión confidencial de video en dispositivos móviles**

17:20-17:40 19. David Mata Mendoza. Instituto Politécnico Nacional. Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacán. Sección de Estudios de Posgrado e Investigación **Ocultamiento de datos reversible en el dominio cifrado de imágenes médicas**

Viernes

10:00-10:20 20. Fernanda D. de Melo Hernández. Universidade Estadual de Maringá, Maringá, PR, Brasil **Sobre idempotentes en anillos conmutativos**

10:20-10:40 21. Daniel Becerra Pedraza. Posgrado en Ciencia e Ingeniería de la Computación. Universidad Nacional Autónoma de México. **Esquema de compartición de secretos con detección eficiente de trampas**

10:40-11:00 22. Rafael Espinosa-García. SEES/Sistemas VLSI, Departamento de Ingeniería Eléctrica, Cinvestav-IPN **Matemáticas y Computación de *Blockchain***

11:00-12:00 Ivelisse Rubio. Departamento de Ciencia de Cómputos, Universidad de Puerto Rico, Río Piedras. **El método de cobertura: un acercamiento intuitivo al cómputo de p-divisibilidad de sumas exponenciales**

12:00-12:40 CAFÉ

12:40-13:00 23. González Rodríguez Florencio Javier. Centro de Investigación en Computación. **Traffic database generation based on TCP scanning techniques for the analysis of the behaviour of a network scan**

13:00-13:20 24. Bruno Ramos Cruz. Coordinación de Ciencias Computacionales, INAOE. **CLIC-ODB: Cell Level Integrity and Completeness for Outsourced Database**

13:20-15:20 COMIDA

15:20-15:40 25. José Rodríguez-Escobar. Centro de Investigación en Matemáticas, A.C. **Firmas digitales estandarizadas y candidatos poscuánticos**

15:40-16:00 26. Elias Javier Garcia Claro. Universidad Autónoma Metropolitana. **Códigos abelianos minimales y sus extrañas dimensiones**

16:00-16:20 27. Daniel Cervantes-Vázquez. Cinvestav - Departamento de computación. **Usando paralelismo en el protocolo SIDH**

16:20-16:40 CAFÉ

16:40-17:00 28. Horacio Tapia-Recillas. Universidad Autónoma Metropolitana-Iztapalapa. **Códigos LCD asociados a ondeletas (wavelets)**

17:00-17:20 29. Juan Josué Gómez Olvera. Instituto Nacional de Astrofísica, Óptica y Electrónica. **Un protocolo seguro de comunicacioń I2I en redes vehiculares, basado en un esquema de secreto compartido**

17:20-17:40 30. Víctor Gabriel Reyes Macedo. Instituto Politécnico Nacional. **Nociones de Seguridad para Sistemas Blockchain**

17:40-18:00 Clausura

Conferencias Magistrales

La Computación Cuántica y la Criptografía

Neal Koblitz

koblitz@uw.edu

University of Washington, USA

Comenzaré con una explicación del algoritmo de Peter Shor, el cual podría factorizar números enteros muy grandes en tiempo polinomial y destruir mucho de la criptografía de clave pública si se pudiera construir una computadora cuántica masiva. Hablaré sobre la comparación entre computadoras y algoritmos clásicos y cuánticos y sobre los obstáculos formidables en la construcción de una computadora cuántica.

Las Criptomonedas

Neal Koblitz

koblitz@uw.edu

University of Washington, USA

Antes de Bitcoin, en los años 1990, existió una forma de criptomonedas muy diferente, el "e-cash" de David Chaum en diferentes versiones. Voy a comenzar con una discusión de las matemáticas de "e-cash" en su versión con curvas elípticas, y después hablar sobre las criptomonedas basadas en cadenas de bloques (*blockchains* en inglés). También describiré los lados positivos y negativos de Bitcoin y otras criptomonedas.

Análisis de la complejidad lineal de arreglos multidimensionales periódicos
(Título corto: Complejidad de Arreglos Multidimensionales)

Ivelisse Rubio

iverubio@gmail.com

Departamento de Ciencia de Cómputos, Universidad de Puerto Rico, Río Piedras

Si se quieren utilizar arreglos en aplicaciones criptográficas, los arreglos deben ser resistentes a ataques y es necesario tener una medida de esa resistencia a ataques. Para sucesiones periódicas (arreglos en una dimensión), la medida de complejidad lineal se define como el grado del polinomio mínimo que genera la sucesión. Es deseable obtener una medida y teoría similar para arreglos multidimensionales que sean consistentes con las de las sucesiones. En este trabajo presentamos una generalización para arreglos multidimensionales de la definición de complejidad lineal y desarrollamos una teoría para estudiarla. Analizamos arreglos construidos con el método de composición y establecemos cotas estrictas para su complejidad lineal.

El método de cobertura: un acercamiento intuitivo al cómputo de p-divisibilidad de sumas exponenciales
(Título corto: p-Divisibilidad de Sumas Exponenciales)

Ivelisse Rubio

iverubio@gmail.com

Departamento de Ciencia de Cómputos, Universidad de Puerto Rico, Río Piedras

La p-divisibilidad de sumas exponenciales se ha usado para caracterizar y demostrar propiedades en la teoría de códigos, criptografía y solubilidad de ecuaciones polinómicas. Una pequeña mejora en el estimado de p-divisibilidad puede tener implicaciones importantes en las aplicaciones. En general, los métodos algebráicos para estimar la p-divisibilidad de sumas exponenciales sobre campos finitos no son elementales. El método de cobertura ofrece una forma intuitiva y elemental para determinar p-divisibilidad que es particularmente conveniente en las aplicaciones. En esta charla daremos una visión general de este método y de cómo puede utilizarse en algunas aplicaciones.

Conferencias por solicitud

1. Network Scan Detection

González Flores Byron
(bgonzlezf@gmail.com)
Centro de Investigación en Computación
Ciudad de México
(Gómez Martínez María Teresa, González Rodriguez Florencio Javier, Pacheco Rodríguez Hugo Sebastian)

This work is a part of a joint project whose objective is to identify if the ports of a computer are being scanned through the use of neural networks.

Port scan is one of the most techniques in a network scan being used to find exposed services that could mean a vulnerability in the network. The process of port scan technique is to send to each of the ports, 65535 ports, a request of connection and refusing it at the moment of the destination accept the connection, using TCP protocol to establish the connection

The Transmission Control Protocol (TCP) is intended for use as a highly reliable host-to-host protocol between hosts in packet-switched computer communication networks, and in interconnected systems of such networks[1].

This work is concentrated in the following flags: source port, destination port, SYN, ACK and RST, that are the fields used to make the request and response to know if the port has a service. In order to identify if the computer is under a port scan, is used a neural network, that has to be able to detect if the equipment is under a scan.

The neural network has to be trained with previously collected network samples with which it will be possible to determine if it is being scanned.The parameters that are given to the neural network are the previously mentioned flags, the neural network will have to return a value that allows us to determine if a port scan is being performed: 0, not scanned, and 1, is scanned.

Referencias

[1] Darpa Internet Program, Protocol Specification, *Transmission Control Protocol*, 1981.

2. Tokenización 101

Laura Natalia Borbolla Palacios

(ln.borbolla.42@gmail.com)

Instituto Politécnico Nacional, ESCOM
Ciudad de México, México

(Trabajo conjunto con Daniel Ayala Zamorano, Sandra Díaz Santiago y Ricardo Quezada Figueroa)

Cuando el comercio a través de Internet comenzó a popularizarse, los fraudes de tarjetas bancarias se convirtieron en un problema grave: según [1], en 2001 se tuvieron pérdidas de 1.7 mil millones de dólares y en 2002 ascendieron a 2.1 mil millones. En este contexto, el PCI-SSC desarrolló un estándar [2], especificando, para negocios en línea, mecanismos de seguridad que protegen los datos sensibles de las tarjetas bancarias en los que es menester proteger la información donde sea que se encuentre en el sistema; empero, este enfoque puede resultar costoso y complicado de realizar, por lo que hace algunos años surgió un nuevo paradigma: la tokenización. Consiste en reemplazar los datos sensibles con valores sustitutos (*tokens*) que no tienen relación alguna con el valor original; mediante este enfoque, la información sensible se concentra en un solo lugar, facilitando la tarea de protección y separando claramente las responsabilidades entre el sistema principal, que opera el negocio, y el sistema tokenizador, que se encarga de la protección de datos sensibles y la comunicación con el entorno bancario. Aunque existen ya compañías proveedoras del servicio de tokenización, esta sigue rodeada de desinformación, pues suelen difundir información imprecisa y cuidan con recelo sus métodos de tokenización. Puesto que todos los algoritmos tokenizadores son distintos, es menester analizar las opciones para utilizar el más apropiado en cada situación.

En esta plática se describirán cinco algoritmos tokenizadores propuestos por la comunidad académica: FFX [3], BPS [4], TKR [5], un DRBG [6] y un algoritmo híbrido reversible [7]. Cabe destacar que el PCI-SSC estableció en [8] una clasificación para los algoritmos: reversibles criptográficos, reversibles no criptográficos, irreversibles autenticables e irreversibles no autenticables; esta clasificación puede resultar un poco confusa, pues aunque un algoritmo utilice varias primitivas criptográficas al tokenizar, termina siendo clasificado como *no criptográfico* si utiliza una base de datos para guardar la relación *token*-tarjeta; por lo que también se propone una nueva clasificación.

Referencias

[1] John S. Kiernan. *Credit Card And Debit Card Fraud Statistics*. Wallethub, 2017. Disponible en:`https://wallethub.com/edu/credit-debit-card-fraud-statistics/25725/`.

[2] Payment Card Industry Security Standards Council. *Data Security Standard - Version 3.2*. 2016. Disponible en: `https://pcicompliance.stanford.edu/sites/g/files/sbiybj7706/f/pci\_dss\_v3-2.pdf`.

[3] Mihir Bellare, Phillip Rogaway y Terence Spies. *The FFX Mode of Operation for Format-Preserving Encryption*. 2010.

[4] Eric Brier, Thomas Peyrin y Jacques Stern. *BPS: a Format-Preserving Encryption Proposal*. 2010.

[5] Sandra Diaz-Santiago, Lil María Rodríguez-Henríquez y Debrup Chakraborty. *A cryptographic study of tokenization systems*. En: Int. J. Inf. Sec. vol. 15, pp. 413-432, 2016. DOI: 10.1007/s10207-015-0313-x. Disponible en: `https://doi.org/10.1007/s10207-015-0313-x`.

[6] Elaine Barker y John Kelsey. *NIST Special Publication 800-90A - Recommendation for Random Number Generation Using Deterministic Random Bit Generators*. 2015. Disponible en: `http://dx.doi.org/10.6028/NIST.SP.800-90Ar1`.

[7] Riccardo Aragona, Riccardo Longo y Massimiliano Sala. *Several proofs of security for a tokenization algorithm*. En: Appl. Algebra Eng. Commun. Comput. vol. 28, pp. 425-436, 2017. DOI: 10.1007/s00200-017-0313-3. Disponible en: `https://doi.org/10.1007/s00200-017-0313-3`.

[8] Payment Card Industry Security Standards Council. *Tokenization Product Security Guidelines – Irreversible and Reversible Tokens*. 2015. Disponible en: `https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf`.

3. Multiplicador RNS en VHDL

José A. Bernal

(jbernal@computacion.cs.cinvestav.mx)

Centro de Investigación y de Estudios Avanzados del IPN
Alcaldía Cuauhtémoc, Ciudad de México

En criptografía es necesario llevar a cabo operaciones de forma rápida y eficiente de modo que sean imperceptibles para el usuario y que no impacten en el rendimiento del equipo, dichas operaciones pueden ser parte de la ejecución de algún protocolo, por ejemplo: establecimiento de llaves *Diffie-Hellman*, firmas digitales, generación de llaves, entre otros. Las operaciones pueden ser: suma, resta y multiplicación, las cuales se llevan a cabo con operandos grandes, es decir, pueden ser números de más de 64 bits.

En los años noventa del siglo pasado, varios autores propusieron el uso del sistema numérico de residuos (*RNS*) como una alternativa para computar aritmética modular sobre operandos grandes. Tomando ventaja del antiguo teorema chino del residuo(*CRT*), la cualidad principal de *RNS* es el representar números enteros muy grandes en términos de un conjunto de enteros pequeños independientes. De esta manera, se intercambia el costo de una sola operación aritmética sobre dos operandos grandes por el cálculo de operaciones modulares independientes más pequeñas que se pueden llevar a cabo en paralelo. Una implementación rápida y eficiente permite llevar a cabo las operaciones en un menor tiempo

y con menor consumo de recursos como pueden ser: energía, memoria, tiempo de CPU, etc.

El diseño en hardware reconfigurable (FPGA *Field programmable gate array*) permite crear dispositivos dedicados que liberan al procesador principal y mejoran los tiempos de ejecución en las operaciones al despojar de algunas tareas que requieren demasiados recursos del procesador. Los dispositivos de hardware reconfigurable permiten diseñar dispositivos dedicados que pueden lograr un mejor rendimiento al ser utilizados en conjunto con dispositivos que no cuentan con los recursos suficientes para llevar a cabo las operaciones en aritmética de números grandes.
Además pueden ser de bajo consumo energético y se pueden acoplar a otros dispositivos que no cuentan con los recursos necesarios para llevar a cabo dichas tareas.

En este trabajo se presenta el diseño de un multiplicador de $64 * 64$ bits a partir de los DSP(*Digital Signal Processing*) que contienen los *FPGAs* modernos, los cuales serán utilizados como base para lograr un dispositivo capaz de llevar a cabo la multiplicación en RNS(*Residue Number System*) para operandos de 128, 256, 512 bits.

El enfoque de esta ponencia se centra principalmente en la implementación tipo diamante y del método de la escuela, ambos en VHDL[1] como el multiplicador base del dispositivo *RNS* final, tomando en cuenta su construcción a partir de los *DSPs* y las características de los mismos.

4. Conjuntos de información a partir de conjuntos de definición para códigos de Reed-Muller de primer y segundo orden

Juan Jacobo Simón Pinero

(jsimon@um.es)

Universidad de Murcia
Murcia, España
(Trabajo conjunto con J. J. Bernal[2])

Resumen: Los códigos de Reed-Muller pueden ser vistos como afín-invariantes para obtener conjuntos de información. Desde este punto de vista, estos códigos pueden ser vistos como códigos cíclicos extendidos (a códigos de grupo) y de este modo, los conjuntos de información del código cíclico es claramente un conjunto de información del código de Reed-Muller; aún más, existe una relación directa entre los conjuntos de definición de ambos códigos. Por otro lado, en [1] introdujimos un método para construir conjuntos de información en códigos abelianos en términos del conjunto de definición. Así, en este trabajo [2] obtenemos conjuntos de información para códigos de Reed-Muller de primer y segundo órdenes vistos como códigos abelianos multivariables.

[1] VHSIC(*Very High Speed Integrated Circuit*) y HDL(*Hardware Description Languaje*)
[2] Universidad de Murcia

Referencias

[1] J. J. Bernal, J. J. Simón: Information sets from defining sets in abelian codes. IEEE Trans. Inform. Theory, vol. 57(12), 7990-7999, 2011.

[2] J. J. Bernal, J. J. Simón: Information sets from defining sets for Reed-Muller codes of first and second order. IEEE Trans. Inform. Theory, vol. 64(10), 6484–6497, 2018.

5. Contrucción de firmas digitales

Pablo Ignacio Soto Blancas

(pablomonki89@gmail.com)

Universidad Autónoma de la Ciudad de México

CDMX

El algoritmo SHA-1 tiene diversas aplicaciones, por ejemplo; seguridad en páginas web, Bitcoin y diversas. En esta plática abordaremos la contrucción de firmas digitales usando funciones hash y su papel que desempeña en el desarollo de la moneda virtual.

Referencias

[1] David, Kravitz., *Digital signature algorithm, Patent Number 5231668.*

[2] Neal, Koblitz., *A Course in Number Theory and Crytography.* Graduate Texts in Mathematics **114**, (1994), Springer-Verlag New York.

6. Implementación de la máquina ENIGMA en LABVIEW

García-Martínez M.

(moises.garcia@tec.mx)

Tecnológico de Monterrey, Escuela de Ingeniería y Ciencias
San Luis Potosí, San Luis Potosí.

(Olais-Govea J. M., Ontañon-García L. J. [3])

La máquina **ENIGMA** es tal vez la máquina electromecánica más famosa de la historia para cifrar y descifrar mensajes, esto se debe principalmente a que fue usada por los nazis durante la segunda guerra mundial y además fue el primer sistema de cifrado

[3] Coordinación Académica Región Altiplano Oeste UASLP, San Luis Potosí, San Luis Potosí.

poli-alfabético, capaz de generar millones de combinaciones haciéndola prácticamente indescifrable.

De forma general el funcionamiento de esta máquina automatiza los cifrados de sustitución, para esto se basa en el uso de tres rotores, cada rotor contiene 26 contactos eléctricos en cada lado y cada contacto de un lado es conectado con el otro extremo de forma aleatoria. Cuando una tecla es presionada, el rotor de la derecha avanza un paso, esto implica que internamente el cableado cambia y da como resultado una nueva letra, es importante mencionar que el cableado interno es diferente para cada rotor y además los rotores son intercambiables. El reflector fue un elemento indispensable y hasta ese momento único en su tipo ya que permitía que la señal eléctrica regresara por los rotores por un camino diferente y de esta forma dar energía al teclado iluminado que muestra el texto cifrado.

El objetivo de este trabajo es poder reconstruir e implementar por medio del software **LABVIEW** el funcionamiento de todos los elementos de esta máquina y lograr el mismo proceso de cifrado-descifrado, así como la interfaz de usuario en el panel frontal.

Referencias

[1] Christof Paar; Jan Pelzl (2009). Understanding Cryptography, Springer.

[2] David H Hamer (1997). Enigma: Actions involves in the 'double stepping' of the middle rotor. Cryptologia 21(1):47-50.

7. Marca de agua híbrida para aumentar la seguridad en ultrasonidos médicos digitales

Diana Nuñez Ramirez

(dian11nurz@gmail.com)

Instituto Politécnico Nacional. Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacán.
Sección de Estudios de Posgrado e Investigación
Av. Santa Ana 1000, Col. San Francisco Culhuacán, C.P. 04430, Ciudad de México,
(Manuel Cedillo Hernández[4])

Resumen:Las necesidades de almacenamiento y manipulación de imágenes médicas digitales surgen como consecuencia de la problemática que presenta el manejo de información radiológica de manera convencional y la generación de grandes volúmenes de datos, el cual, ocasiona una pérdida del 20 % de las imágenes médicas y da origen a inconsistencias en el diagnóstico médico [1]. Para enfrentar este problema surge el estándar DICOM

[4]Instituto Politécnico Nacional. Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacán. Sección de Estudios de Posgrado e Investigación

(Digital Imaging and Comunication in Medicine) que es un mecanismo de codificación, almacenamiento y transmisión de imágenes médicas digitales en formato dcm[2].
La seguridad de la información médica requiere de tres características obligatorias: confidencialidad, confiabilidad y disponibilidad. El método propuesto busca reforzar la confidencialidad, la cual indica que solo personal autorizado tiene acceso a información específica bajo condiciones controladas y la confiabilidad, la cual está conformada por dos importantes aspectos: la integridad, encargada de verificar que la información del paciente no está modificada y la autenticación que garantiza que la información del paciente es correcta y proviene de una fuente fidedigna.[3].
Se propone un método híbrido de marca de agua aplicado a imágenes DICOM en la modalidad de ultrasonido, que integra dos marcas de agua, una invisible y otra visible-imperceptible. El almacenamiento de manera separada del Registro Electrónico del Paciente (EPR, por sus siglas en inglés) y las imágenes médicas puede conducir a una desvinculación entre estos dos archivos, con el fin de evitar este problema se propone una marca de agua invisible basada en el dominio de la transformada discreta de Fourier (TDF) a través del Acceso Múltiple por División de Código de Secuencia Directa (DS-CDMA, por sus siglas en inglés), la cual inserta una secuencia de bits generada por el resumen criptográfico RIPEMD 160 en las frecuencias medias de la TDF. Finalmente se inserta una marca de agua visible-imperceptible basada en el dominio espacial que inserta un logotipo binario sin alterar significativamente la calidad visual de la imagen con el propósito de verificar su autenticidad.Este método garantiza disminuir los errores diagnósticos provocados por corrupción de datos o modificaciones intencionales en información médica y radiológica que afecten la salud del paciente.
La imperceptibilidad del método es evaluada con el Índice de Relación Pico Señal-Ruido (PSNR) y el Índice de Similitud Estructural (SSIM), por otro lado, la robustez frente a diferentes distorsiones es medida con la Tasa de Bits Erróneos (BER) para la marca de agua invisible y la legibilidad del logotipo en imágenes marcadas ante ataques de compresión, filtrado, ruido y distorsiones geométricas para la marca de agua visible-imperceptible.

Referencias

[1] Gutiérrez Martínez, J. et. al. *Sistema PACS-CNR, una propuesta tecnológica.* Revista Mexicana de Ingenierá Biomédica, [S.l.], v. 24, n. 1, p. 77-85, mar. (2003).

[2] Coatrieux G., Maître H., Sankur B., Rolland Y., Collorec R. *Relevance of watermarking in medical imaging* IEEE-embs Information Technology Applications in, Biomedicine, pp. 250– 255 (2000).

[3] A. F. Qasim, Farid Mezianea, Rob Aspina. *Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review.* Computer Science Review 27 45–60, (2018).

8. Polinomios básicos primitivos y representaciones de elementos en un anillo de Galois

Juan Carlos Ku Cauich

(jcku@cs.cinvestav.mx)

Departamento de Computación, Centro de Investigación y de Estudios Avanzados del IPN
07360 Ciudad de México

(Trabajo conjunto con el Dr. Guillermo Morales Luna[5])

Un anillo de Galois es un anillo finito con identidad tal que los divisores de cero y el cero conforman el ideal $\langle p \rangle$, donde p es el número primo tal que para un entero $s \in \mathbb{Z}^+$, p^s es la característica del anillo. Para cada $m \in \mathbb{Z}^+$, la función

$$\pi_p : \mathbb{Z}_{p^s}[X] \to \mathbb{F}_p[X] \ , \ g(X) = \sum_{j=0}^{m-1} a_j X^j \mapsto g(X) \text{ mód } p = \sum_{j=0}^{m-1} (a_j \text{ mód } p) X^j,$$

es un anillo de homomorfismos. Un polinomio $g(X) \in \mathbb{Z}_{p^s}[X]$ de grado m es básico irreducible (primitivo) si $\pi_p(g(X))$ es irreducible (primitivo) en $\mathbb{F}_p[X]$. En tal caso, $\mathbb{Z}_{p^s}[X]/\langle g(X) \rangle$ es un anillo de Galois denotado $GR(p^s, m)$ y hay un elemento $\xi \in GR(p^s, m)$ tal que $o(\xi) = p^m - 1$, $g(\xi) = 0$, de modo que las siguientes expresiones se cumplen:

- Forma aditiva: $GR(p^s, m) = \mathbb{Z}_{p^s}[\xi] = \sum_{j=0}^{m-1} a_j \xi^j, \quad a_j \in \mathbb{Z}_{p^s}$.
- Forma p-ádica: $\sum_{k=0}^{s-1} b_k p^k, \quad b_k \in \mathcal{T}(g(X))$, donde $\mathcal{T}(g(X)) = \{0\} \cup (\xi^i)_{i=0}^{p^m-2}$ es el conjunto de Teichmüller.

Sea un polinomio mónico primitivo $f_{pm}(X) \in \mathbb{F}_p[X]$ divisor de $P_{pm}(X) = X^{p^m-1} - 1$ en $\mathbb{F}_p[X]$. Por el levantamiento de Hensel hay un único polinomio mónico básico primitivo $f_{psm}(X) \in \mathbb{Z}_{p^s}[X]$ divisor de $P_{pm}(X)$ en $\mathbb{Z}_{p^s}[X]$ tal que $\pi_p(f_{psm}(X)) = f_{pm}(X)$. Así, una correspondencia natural $f_{pm}(X) \leftrightarrow f_{psm}(X)$ se da para cada s. En el peor de los casos, para valores pequeños de m y s la búsqueda del polinomio correspondiente al levantamiento de Hensel puede hacerse de manera exhaustiva. Alternativamente una lista de polinomios mónicos primitivos en el anillo $\mathbb{F}_p[X]$ puede ser consultada con el fin de considerar la imagen inversa bajo la proyección módulo p.

En este trabajo presentamos procedimientos básicos para obtener el levantamiento de Hensel de polinomios primitivos y sus respectivas implementaciones. Encontrar estos polinomios básicos permite representar de manera exacta los elementos de un anillo de Galois en forma aditiva y p-ádica. Encontrar la forma p-ádica de un elemento de un anillo de Galois es como una extensión del problema del logaritmo discreto sobre campos finitos pues los coeficientes de esta forma presentan instancias del problema. Aplicaciones de este problema sobre campos finitos se encuentran por ejemplo en el criptosistema ElGamal y en el intercambio de llaves de Diffie-Hellman.

[5]Departamento de Computación, Centro de Investigación y de Estudios Avanzados del IPN

9. Diseño en hardware de un cifrador ligero

Joel López Romero

(jllpzrmr7@gmail.com)

Instituto Politénico Nacional - ESCOM
Ciudad de México

(César Cruz, Eric López, Nayeli Vega, Sandra Díaz)

Debido a la miniaturización de los componentes electrónicos, en los últimos años se han desarrollado dispositivos de tamaño milimétrico, y con ello han surgido nuevas tecnologías. Una aplicación de éstas son los aparatos que utilizan IoT, cada vez más comunes y los cuales generan datos valiosos de nuestra vida diaria, como frecuencia cardiaca, distancia recorrida, la temperatura de nuestro hogar, etc [1, 2]. Desafortunadamente, los datos enviados por estos dispositivos pueden ser interceptados, y en el caso de no poseer algún mecanismo que permita proteger su confidencialidad, estos pueden quedar comprometidos [3, 4]. En la actualidad, existen diversos algoritmos de cifrado, como AES o RSA. Infortunadamente, estos algoritmos han sido desarrollados para su uso en computadoras de escritorio o servidores, lo cual hace difícil (o incluso imposible) implementarlos en ambientes restringidos, es por ello que surge la criptografía ligera.

La criptografía ligera es una rama de la criptografía que se enfoca en proveer soluciones para dispositivos restringidos en recursos [5]. Hay una gran cantidad de trabajo realizado por la comunidad académica acerca de la criptografía ligera, es por ello que se realizó una investigación y análisis de varios cifradores ligeros existentes. Con base en el resultado de la investigación, se llegó a la elección del algoritmo ANU-II [6], que se diseñará en hardware. Este cifrador provee un nivel de seguridad aceptable y su implementación en hardware es relativamente pequeña. La ventaja de este algoritmo de cifrado es que aún no existen ataques que prueben que sea vulnerable, además de que sus implementaciones en hardware son más pequeñas que la de otros algoritmos. Por otra parte, las realizadas para este cifrador no están diseñadas completamente en hardware, por lo que no son aprovechadas las ventajas que el diseño digital ofrece, como el paralelismo y la lógica combinacional.

Partiendo del algoritmo elegido y siguiendo el proceso de diseño de un sistema digital, se crearón cartas ASM, las cuales permiten observar las instrucciones que conforman el algoritmo desde una perspectiva de hardware, identificando cuales se pueden paralelizar o mejorar. Posteriormente, se continuó con el diseño de las arquitecturas y sus componentes.

Usando una metodología Top-Down, se proponen dos arquitecturas enfocadas en dos aspectos importantes de la criptografía ligera: uso de memoria y tiempo de ejecución, aprovechando al máximo las ventajas que el diseño digital ofrece, para así poder reducir el consumo de recursos del algoritmo en hardware.

Referencias

[1] Statista. (2016) Internet of things (iot) connected devices installed base worldwide from 2015 to 2025 (in billions). [Online]. Available: https://goo.gl/tBj3wY

[2] A. K. S. et. al. (2018) A survey on sensor-based threats to internet-of-things (iot) devices and applications. [Online]. Available: https://arxiv.org/pdf/1802.02041.pdf

[3] Infosys. (2018) Wearable devices in banking. [Online]. Available: https://goo.gl/RJFKAU

[4] Bitdefender. (2014) Bitdefender research exposes plain-text android wearable devices communication. [Online]. Available: https://www.youtube.com/watch?v=utVnrq5uCuM

[5] K. A. M. et.al. (2017) Report on lightweight cryptography. [Online]. Available: https://goo.gl/KcXQa8

[6] D. Vijay, B. Gaurav, and P. Jagdish, "Anu–ii: A fast and efficient lightweight encryption design for security in iot," IEEE , 2017. [Online]. Available: https://ieeexplore.ieee.org/document/8336586

10. De la búsqueda de raíces polinómicas

Jesús Javier Chi Domínguez
(jjchi@computacion.cs.cinvestav.mx)

Cinvestav IPN, Departamento de computación
Unidad Zacatenco, Ciudad de México
(Trabajo conjunto con Francisco Rodríguez Henríquez)

Dado un polinomio f de grado d con coeficientes sobre un campo finito de q^ℓ elementos. El problema de la búsqueda de raíces de f es definido como el problema de hallar todas las raíces de f. Dicho problema puede ser visto como una instancia muy especial del problema de la factorización polinómica (es decir, factorizar f). Como sea, los mejore algoritmos de factorización y búsqueda de raíces están, mayormente, basados en los algoritmos de Berlekamp [1, 2] y Cantor-Zassenhaus [3], los cuales tienen una complejidad de $\tilde{O}\big(d^3 + \log(q^\ell) \cdot d^2\big)$ y $\tilde{O}\Big(d^2 \cdot \log(q^\ell)\Big)$ [6], respectivamente (para un mayor detalle, léase [4]).

Definición 1 (Polinomios bajo la acción de Frobenius)**.** *Sean p, ℓ y n tres números enteros positivos tales que p es un número primo, $(n, \ell) = 1$, y $n, \ell > 1$. Sea $\mathbb{F}_q$ un campo finito con $q = p^n$ elementos, y $\mathbb{F}_{q^\ell}$ una extensión de grado ℓ del campo $\mathbb{F}_q$. Entonces, para cada polinomio $h = \sum_{i=0}^{d} h_i x^i \in \mathbb{F}_p[x]$, se define $h^\sigma(x) = \sum_{i=0}^{d} h_i \cdot x^{(q^i)}$.*

Claramente, $p(x) = x^\ell + 1$ implica que $h^\sigma(x) = x^{q^\ell} + x$ tiene todas sus raíces en $\mathbb{F}_{q^\ell}$. Como consecuencia, cualquier factor polinómico $h(x) \in \mathbb{F}_p[x]$ of $(x^\ell + 1)$ de grado d satisface que el polinomio $h^\sigma(x)$ de grado q^d se escinde en factores lineales sobre $\mathbb{F}_{q^\ell}$. De lo cual, hallar todas las raíces de $h^\sigma(x)$ se vuelve impráctico cuando q^d es lo suficientemente grande.

Teorema 1 (Resultado principal)**.** *Es posible obtener todas las raíces, que habitan en $\mathbb{F}_{q^\ell}$, del polinomio $h^\sigma(x)$ con aproximadamente $\Big(2\ell + d \cdot (\ell - 1) \cdot n \cdot \log_2(p)\Big)$ multiplicaciones, $\frac{d \cdot (\ell-1) \cdot n \cdot \log_2(p)}{2}$ cuadrados y $\big[(\ell - 1)(2d - 1) + \ell \cdot q^d\big]$ adiciones en $\mathbb{F}_{p^\ell}$.*

[6] $\tilde{O}\big(g(n)\big)$ se refiere a $O\Big(g(n) \cdot \big(\log g(n)\big)^k\Big)$ para algún número entero k

Referencias

[1] E. R. Berlekamp. *Factoring polynomials over finite fields.* The Bell System Technical Journal, 46(8):1853-1859, 1967.

[2] E. R. Berlekamp. *Factoring Polynomials Over Large Finite Fields.* Mathematics of Computation, 24(111):713-735, 1970.

[3] David G. Cantor and Hans Zassenhaus. *A New Algorithm for Factoring Polynomials Over Finite Fields.* Mathematics of Computation, 36(154):587-592, 1981.

[4] Joachim von zur Gathen and Daniel Panario. *Factoring Polynomials Over Finite Fields: A Survey.* Journal of Symbolic Computation, 31(1):3-17, 2001.

11. Criptoanálisis físico contra dispositivos electrónicos embebidos, y su protección

Carolina Jeanette Villaseñor Rodelas[1], David Tinoco Varela[2]

[1]carolvr@live.com.mx, [2]dativa19@hotmail.com

Universidad Nacional Autónoma de México, FES Cuautitlán.
[1] Licenciatura en Tecnología, [2]Departamento de Ingeniería-ITSE.

Hoy en día son realizados millones de movimientos electrónicos diariamente, estos pueden ser transacciones comerciales y económicas, intercambio de datos políticos y sociales, e incluso, comunicaciones personales entre dos usuarios. Con la finalidad de proteger cada uno de estas transferencias de información, se han creado diversos sistemas criptográficos, tal como RSA (Rivest, Shamir, Adleman). Estos algoritmos garantizan la seguridad de los datos transmitidos y por lo tanto dan la confianza a los usuarios de poder realizar intercambio de información de forma segura.

Actualmente, son utilizados algoritmos de encriptación de datos seguros y confiables, por ejemplo RSA, que para romper su seguridad con los avances matemáticos, algorítmicos y computacionales con los que contamos hoy en día, necesitaríamos un tiempo de ejecución de miles de millones de años. Sin embargo, aunque estos algoritmos son teóricamente seguros, cuando ellos son implementados en dispositivos electrónicos tal como un sistema embebido, se presentan vulnerabilidades relacionadas directamente con la implementación.

Cada vez que un algoritmo es ejecutado dentro de un sistema embebido o electrónico, se generan emanaciones físicas tales como el consumo de potencia o emanación térmica, que pueden ser registradas por dispositivos de medición tal como un osciloscopio. Cada una de estas emanaciones presenta una firma particular dependiendo del dato que se está procesando, de esta forma, es posible analizar tales señales y obtener información relacionada a la clave privada del sistema criptográfico ejecutado en tal dispositivo.

Este proyecto, pretende mostrar las amenazas a las que son expuestos los diferentes dispositivos electrónicos tales como sistemas embebidos, microcontroladores y microprocesadores, cuando ellos ejecutan sistemas criptográficos y las técnicas algorítmicas utilizadas para evitar tales vulnerabilidades. Centrándonos principalmente en el uso de algoritmos de exponenciación modular, y sus formas regulares. Se presenta un proyecto de gran importancia para el diseño de

interfaces que puedan ser conectadas a esquemas tecnológicos como el Internet de las Cosas.

Palabras clave: Criptoanálisis, algoritmos de exponenciación modular, sistemas embebidos.

12. Códigos polares sobre Curvas Castillo

Eduardo Camps Moreno
(ecfmd@hotmail.com)
ESFM-IPN
CDMX

Resumen: Dada una matriz G, se toma G_n como una permutación de renglones de $G^{\otimes n}$, donde $\otimes$ representa el producto tensorial. Se eligen los mejores renglones de G_n para la transmisión sobre un canal W y al conjunto de sus índices le denominamos $\mathcal{A}_n$. Un código polar $C_{\mathcal{A}_n}$ es el generado por los renglones de G_n indexados por $\mathcal{A}_n$. La estructura de $\mathcal{A}_n$ es de particular interés para la descripción del código.

Retomando las ideas de Bardet et. al. en [2], tomamos una curva algebraica $(\mathcal{X}, Q)$ tipo Castillo sobre $\mathbb{F}_q$ y probamos que sobre el canal q-ario simétrico, la matriz G_n se puede describir en términos de un orden monomial derivado del semigrupo de Weierstrass $H(Q)$ y que la estructura de $H(Q)$ permite garantizar información sobre $\mathcal{A}_n$, además de describir el dual y aproximar la distancia mínima.

Referencias

[1] Arikan, E. (2008, July). Channel polarization: A method for constructing capacity-achieving codes. In 2008 IEEE International Symposium on Information Theory (pp. 1173-1177). IEEE.

[2] Bardet, M., Dragoi, V., Otmani, A., & Tillich, J. P. (2016, July). Algebraic properties of polar codes from a new polynomial formalism. In 2016 IEEE International Symposium on Information Theory (ISIT) (pp. 230-234). IEEE.

[3] Camps, E., Martínez-Moro, E., & Sarmiento, E. (2019). Vardøhus Codes: Polar Codes Based on Castle Curves Kernels. arXiv preprint arXiv:1901.06923.

13. Generación de S-Boxes usando la ecuación logística

Luis Roberto Nava Lara, Marco Antonio Rubio Cortés

(luisrobertonavalara@gmail.com, ma.rubiocor@outlook.com)

Escuela Superior de Cómputo - IPN
Lindavista, Ciudad de México
(Dr. Benjamín Luna Benoso, Dr. Víctor Manuel Silva García [7])

Resumen: en este documento se presenta una alternativa para la generación de cajas de sustitución (***S-Box***, por su término en inglés) con alta no linealidad, de hecho, superior a todas las cajas de sustitución del algoritmo de cifrado DES.

La generación del caos se realiza mediante la ecuación logística, debido a su comportamiento dinámico y caótico, para generar un número aleatorio con al menos 768 dígitos. Posteriormente se aplica un algoritmo para generar una permutación que nos sirve de base para construir la caja de sustitución.

Aplicando el cálculo de la no linealidad se filtran y obtienen aquellas cajas con un valor mayor a 96. Realizando corrimientos hacia la izquierda de la caja de sustitución se busca una caja con no linealidad de 108 (ver fig. 1), la cual nos da un porcentaje de no linealidad de 84.37 %.

Como resultado de la investigación se dará a conocer toda la información estadística obtenida durante el proceso de generación de la caja de sustitución a través de este método.

38	a5	ff	94	9	e9	b7	4a	f5	5e	1f	98	8e	86	d1	fd
66	91	0	65	72	28	9a	6b	e7	c5	85	df	68	6a	45	ec
a3	fe	c9	e8	8f	f6	4c	56	f7	3c	93	5b	a6	e2	6f	57
23	cb	d4	ee	48	3a	e4	b2	40	80	88	89	cf	bb	51	ac
81	6	43	ce	90	bd	9c	bf	4e	3d	d7	b0	79	b5	e0	49
d	6d	c7	9d	b4	8a	70	18	96	19	73	26	47	31	5d	a2
63	da	d5	c4	4b	9b	67	95	3e	77	2e	74	76	97	f4	a1
8d	78	5a	7c	3f	7d	44	d9	ca	b6	a	62	dd	82	2b	7f
71	f1	4f	f9	de	a8	e	61	34	b9	53	59	f8	a9	14	41
ea	3b	1e	ae	c1	9f	f2	be	37	5	c6	5c	dc	c8	9e	1d
2d	2	2f	e1	87	fa	a0	b	16	fc	30	a7	1a	af	84	d8
cc	4d	22	12	d6	75	32	6e	83	52	5f	eb	aa	7e	46	d0
f3	10	25	11	33	92	f0	fb	7b	69	ba	58	bc	c2	1	55
39	54	b1	f	8b	29	e6	e3	d2	8c	8	42	b8	a4	c0	2a
c3	13	99	ed	4	ef	ab	36	21	e5	35	d3	1b	cd	7	6c
7a	24	17	15	60	b3	ad	c	50	27	2c	3	db	1c	20	64

Figura 1: Caja de sustitución generada

12	ce	a1	fb	e4	99	41	ee	da	4	7a	a7	f7	50	86	d3
c1	c3	b3	e1	8e	f3	a8	f2	57	59	ac	ec	fd	9f	92	a
fe	e8	b2	30	f1	c2	5b	f9	15	d5	df	7e	fa	a0	6a	a2
aa	5d	b6	c4	88	ea	e7	98	0	d0	35	91	29	49	68	74
38	8f	db	42	76	1e	be	5c	34	4f	7	64	26	b1	48	82
f8	3e	b9	8a	d1	cf	27	2f	cb	8b	72	2b	9b	5e	9	ba
f4	87	7b	60	ff	13	10	66	1c	c9	1d	17	ef	51	b7	2e
56	80	14	5a	6b	b5	6c	69	71	4c	f0	c8	73	75	bd	7f
39	40	7d	b8	ae	1a	d	a4	3a	3b	55	d4	d9	70	c	24
44	11	c5	2a	3	67	58	6d	b	e2	16	65	46	53	9e	95
a6	6f	5f	20	dd	1	2c	ab	85	8d	bc	e6	3f	f6	93	ad
4b	d2	37	f5	54	4d	79	6	dc	89	ca	3d	cc	45	97	47
de	94	cd	e0	63	19	9a	52	9d	22	78	31	b0	ed	43	3c
bf	e	d8	eb	32	62	b4	4a	af	77	61	fc	9c	7c	84	1b
4e	a3	2d	d7	36	e9	d6	18	23	5	90	bb	1f	e3	33	e5
c6	81	96	c0	6e	8	25	28	8c	83	a5	c7	a9	f	21	2

Figura 2: Caja de sustitución inversa

[7] Centro de Innovación y Desarrollo Tecnológico en Cómputo - IPN, C.P. 07700. Nueva Industrial Vallejo, Ciudad de México

14. BlockChains y sus aplicaciones

José de Jesús Angel Angel
jjaa@math.com.mx
Universidad Anáhuac
Huixquilucan, Estado de México

Desde la invención de la criptografía de clave pública; que hizo que el dominio de la tecnología criptográfica se extendierá de la industria militar y diplomática a la industria financiera y comercial, no había visto otro gran paso, hasta hace pocos años con el descubrimiento de la moneda BitCoin. Particularmente por su esquema de BlockChains, que ha resultado muy adaptable a diferentes aplicaciones. En esta plática damos una revisión de los BlockChains desde su aparición con BitCoin hasta las múltiples aplicaciones en diferentes industrias.

Referencias

[1] Blockchains, M. Swan, O'Reilly Media, Inc. 2015.

[2] Mastering Blockchains, A. M. Antonopoulos, O'Reilly Media, Inc. 2017.

[3] Understanding Bitcoin, P. Franco, Wiley 2015.

[4] Business Innovation Though Blockchain, V. Morabito, Springer 2017

15. Cifrado basado en álgebras de conglomerado

Leticia Peña Téllez
(lpenat@uaemex.mx)
Facultad de Ciencias UAEMéx
Toluca, Estado de México
(Trabajo conjunto con Martin Ortiz Morales[8])

Las álgebras de conglomerado fueron introducidas por S. Fomin y A. Zelevinsky en el año 2002 (cf. [1]), mismos que dieron una clasificación de las álgebras de conglomerado de tipo finito (cf. [2]), el cual puede resumirse como: una álgebra de conglomerado es de tipo finito (denotaremos como $\mathcal{A}_r$) si y sólo si la parte principal de una semilla visto como un carcaj valuado es una gráfica valuada correspondiente a un diagrama de Dynkin (cf. [3]), $\mathcal{A}_r$ corresponde a un diagrama de Dynkin Γ con r vértices. Se establece una relación entre la base de un campo finito $\mathbb{F}_q$ visto como un $\mathbb{Z}_p$-espacio vectorial y los elementos de un conglomerado inicial en $\mathcal{A}_r$; donde $q = p^r$, p es un número primo y r es el número de vértices del diagrama de Dynkin Γ y el grado de un polinomio $f(x)$ irreducible sobre $\mathbb{Z}_p[x]$ tal que $\mathbb{F}_q \cong \mathbb{Z}_p[x]/\langle f(x)\rangle$. Esta representación nos permite ver un mensaje m como elemento de un campo finito y como una combinación lineal de elementos del conglomerado inicial. Se propone cifrar el mensaje m utilizando como clave

[8] Facultad de Ciencias UAEMéx

$k = \{k_0, k_1, \ldots, k_t\}$, donde cada k_i es un entero entre 0 y $r-1$ que satisface ciertas condiciones y los números $k_1, \ldots, k_t$ representan las direcciones en las que se realizan mutaciones sucesivas en $\mathcal{A}_r$. El mensaje cifrado c se puede ver como un elemento del conglomerado obtenido al finalizar la sucesión de mutaciones. Se mostrará con un ejemplo como cifrar y descifar un mensaje usando una álgebra de conglomerado de tipo finito, todas las operaciones y mutaciones del ejemplo son hechas con ayuda de un paquete para álgebras de conglomerado en Sage (cf. [4]).

Referencias

[1] S. Fomin y A. Zelevinsky. Cluster algebras. I. Foundations. *J. Amer. Math. Soc.* 15 (2002), no. 2, 497-529.

[2] S. Fomin y A. Zelevinsky. Cluster algebras. II. Finite type classification. *Invent. Math.* 154 (2003), no. 1, 63-121.

[3] K. Erdmann y M.J. Wildon. Introduction to Lie Algebras. Springer Undergraduate Mathematics Series. 2006.

[4] G. Musiker y C.Stump. A compendium on the cluster algebra and quiver package in Sage. *Sém. Lothar. Combin.*65 (2010/12), Art. B65d, 67pp.

16. Matrices L-G y Teoría de Códigos

Dr. Jesús Carrillo Pacheco

jesus.carrillo2357@gmail.com

Academia de Matemáticas
Universidad Autónoma de la Ciudad de México

El objetivo de esta charla es presentar una familia de matrices que nos:

1) Permita establecer propiedades geométricas de la variedad Lagrangiana-Grassmannian.

2) Definir códigos LDPC.

3) Definir turbo códigos.

4) Definir códigos Lagrangianos-Grassmannianos.

17. Neural Networks Applied to Network Scan Detection

Hugo Sebastian Pacheco Rodríguez
(huropacheco@gmail.com)
Centro de Investigacíon en Computaciíon
Ciudad de Mexico
(Gómez Martínez María Teresa, González Flores Byron, González Rodriguez Florencio Javier)

While there are Machine Learning algorithms enough powerful to predict the behaviour of computer networks, also exist cases that cannot be predicted by classical Machine Learning algorithms. A good example of this is Network Scan where the behaviour of the scan depends directly on the counterparts, they can change the way to scan the network in order to avoid being blocked, this makes the data vary without in some cases without any relationship. In other words, the relationships between inputs and outputs are non-linear and complex, Neural Networks have the ability to model these non-linear and complex relationships[1].

Also, we chose to use Neural Networks because there is not restriction on the input variables, our data could be distributed as we want and the amount of collected data depended only on the parameters of which the Neural Network learned. The goal of use Neural Networks was generate an efficient model capable to detect the relationship between the oscillation of information contained in TCP header to detect a network scan.
In order to classify network scans, the created neural network have 6 input features previously studied and selected that characterize a network scan. The output of the neural network is binary (1 - scanned and 0 - no scanned).

Referencias

[1] Jie Zhou, Ganqu Cui, Zhengyan Zhang, Cheng Yang, Zhiyuan Liu, Lifeng Wang, Changcheng Li and Maosong Sun. Graph Neural Networks: A Review of Methods and Applications, 2018; arXiv:1812.08434.

18. Transmisión confidencial de video en dispositivos móviles

Néstor Alejandro Ramírez García
(aramirezgarcia8@gmail.com)
Instituto Politécnico Nacional, ESCOM
Ciudad de México, Ciudad de México
(Sandra Díaz Santiago, Blanca E. Carvajal Gámez)

Resumen:
Los dispositivos móviles en la actualidad son una herramienta utilizada en la captura de videos; cuando estos videos contienen información sensible que necesita transmitirse, es necesario proponer un método que garantice la confidencialidad, esto con el fin de que solo el usuario autorizado pueda tener acceso al contenido.

Este trabajo propone un método que integra dos tipos de estrategias de seguridad informática encargadas de proveer confidencialidad: criptografía y esteganografía, ambas estrategias se aplican a archivos de video y serán implementadas en un dispositivo móvil. El objetivo es mantener una compensación entre el nivel de seguridad y la calidad del video en un dispositivo móvil. En la parte criptográfica, se trabaja con archivos de video comprimidos bajo el protocolo H.264 y se implementan dos de las técnicas empleadas para el cifrado de video; se cifra un archivo de video completo utilizando criptografía ligera y también se hace uso de algoritmos selectivos, es decir; solo se cifran los iframes. El archivo cifrado se oculta dentro de otro archivo de video *.avi que maneja una compresión sin pérdidas; este proceso se hace mediante el uso de la esteganografía en dominio espacial y frecuencial.

19. Ocultamiento de datos reversible en el dominio cifrado de imágenes médicas

David Mata Mendoza
(dmatam1000@gmail.com)
Instituto Politécnico Nacional. Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacán.
Sección de Estudios de Posgrado e Investigación
Avenida Santa Ana 951, San Francisco Culhuacan, Culhuacan CTM V, 04260 Ciudad de México, CDMX, México
(Trabajo conjunto con Manuel Cedillo Hernández[9] y Mariko Nakano Miyatake[9])

En los últimos años se han implementado Sistemas de Archivado y Transmisión de Imágenes (PACS) en el área médica, con el fin de almacenar y distribuir imágenes médicas de forma más eficiente; mientras que la administración de dichas imágenes e información asociada es gestionada por el estándar de Imagenología Digital y Comunicación en Medicina (DICOM), el cual provee los protocolos de comunicaciones para transmisión de información médica, así como las especificaciones técnicas de archivo correspondientes a los datos almacenados [1]. Sin embargo, la expansión de la imagenología digital en el campo de la medicina ha aumentado la necesidad de garantizar la integridad y seguridad de estas imágenes, ya que contienen información confidencial del paciente que puede ser utilizada en fraudes de seguros médicos, robo de identidad, entre otras actividades ilegales. Con la finalidad de proteger la privacidad de una imagen médica, así como la información personal del paciente asociada a ella, en este trabajo se propone un esquema de ocultamiento de datos reversible [2] en imágenes médicas cifradas que permite la extracción de los datos y la restauración de la región de interés (ROI)[3], ya sea a partir del dominio espacial o bien del dominio cifrado de la imagen en cuestión. En la etapa de inserción, la imagen es re-ordenada en un apilamiento de la región de no interés (RONI) y ROI seleccionadas, para posteriormente cifrar la imagen utilizando el cifrador de flujo AES en su modalidad CTR o bien OFB. Para propósitos de este proyecto, en la RONI se insertan los bits menos significativos (LSB) de la ROI original concatenados con los metadatos que contienen información del paciente, como nombre, fecha de nacimiento y género, así como con el resumen del diagnóstico del paciente, mediante la técnica de LSB Replacing. Por otro lado, en la ROI se insertan resúmenes criptográficos, generados con el algoritmo SHA-512, que permiten comprobar la integridad de

[9]Instituto Politécnico Nacional. Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacán. Sección de Estudios de Posgrado e Investigación

los datos insertados en la RONI, así como de la ROI recuperada. Finalmente, el receptor podrá obtener una imagen aproximada al descifrar directamente la imagen cifrada con los datos insertados al tener la llave de cifrado; o bien extraer sin error los datos insertados, ya sea de la imagen cifrada o de la aproximación, con la llave de inserción; y en caso de tener ambas llaves, podrá recuperar exactamente la ROI y datos insertados sin pérdida. Para las pruebas experimentales de este esquema se utilizaron Tomografías Computarizadas (CT) con dimensiones de 512 x 512 pixeles y una resolución de 12 bits, en formato DICOM, donde la Relación Señal Ruido Pico (PSNR) e Índice de Similitud Estructural (SSIM) de las imágenes aproximadas y recuperadas demuestran que la calidad visual de la imagen no resulta realmente afectada [4], aun cuando se utilizan diferentes tasas de inserción.

Referencias

[1] Coatrieux, G., Maître, H., Sankur, B., Rolland, Y., Collorec, R.: Relevance of watermarking in medical imaging. In: IEEE-embs Information Technology Applications in, Biomedicine, pp. 250–255 (2000).

[2] Y. Shi, X. Li, X. Zhang, H. Wu and B. Ma, Reversible data hiding: Advances in the past two decades,ïn IEEE Access, vol. 4, pp. 3210-3237, 2016. doi: 10.1109/ACCESS.2016.2573308.

[3] Liu, Yuling, Xinxin Qu and Guojiang Xin. "A ROI-based reversible data hiding scheme in encrypted medical images." J. Visual Communication and Image Representation 39 (2016): 51-57. doi: 10.1016/ j.jvcir.2016.05.008.

[4] Wang, Z., Bovik, A.C., Sheikh, H.R., Simoncelli, E.P.: Image quality assessment: from error visibility to structural similarity. IEEE Trans. Image Process. 13(4), 600–612 (2004)

20. Sobre idempotentes en anillos conmutativos

Fernanda D. de Melo Hernández

(fdmelo@uem.br)

Universidade Estadual de Maringá
Maringá, PR, Brasil

(Trabajo conjunto con Cesar A. Hernández Melo [10] y Horacio Tapia-Recillas[11])

Resumen: Un elemento idempotente e en un anillo R tiene la sencilla propiedad de que $e^2 = e$. Este tipo de elemento ha sido estudiado en varias áreas de las matemáticas, por ejemplo en teoría de representaciones en la descomposición de módulos y en la teoría de la información, ya sea para describir códigos lineales, o para estudiar propiedades especificas de un código.

Describir tales elementos no siempre es una tarea fácil. Una forma de hacerlo es via levantamiento. A groso modo, este método consiste en describir los elementos idempotentes de un anillo R a partir de los elementos idempotentes de un anillo cociente R/N, donde N es un ideal

[10] Universidade Estadual de Maringá, PR, Brasil
[11] UAM-Iztapalapa, CDMX, Mexico

de R. Mas precisamente, fue demostrado en [1, Proposition 7.14, pag.405] que, si N es un ideal nil de un anillo conmutativo R y $\bar{f}$ es un elemento idempotente en R/N, entonces

$$e = \sum_{i=n}^{2n-1} \binom{2n-1}{i} f^i (1-f)^{2n-1-i}. \tag{1}$$

es el unico elemento idempotente en R tal que $\bar{e} = \bar{f}$.

En esta charla mostraremos que sobre ciertas condiciones el idempotente levantado e asociado a $\bar{f}$ dado en (1) puede ser calculado como una potencia de f en el anillo R. Como aplicación de este resultado, describiremos los idempotentes de un anillo de grupo conmutativo RG, donde R es un anillo de cadena.

Referencias

[1] N. Jacobson, *Basic II.* W. H. Freeman and Company, New York, 1989.

21. Esquema de compartición de secretos con detección eficiente de trampas

Daniel Becerra Pedraza

bpd18@uxmcc2.iimas.unam.mx

Posgrado en Ciencia e Ingeniería de la Computación
Universidad Nacional Autónoma de México

Gerardo Vega Hernández

gerardov@unam.mx

Dirección General de Cómputo
y de Tecnologías de Información y Comunicación
Universidad Nacional Autónoma de México

El trabajo a exponer es un artículo presentado recientemente el 28 de marzo del presente año en "The 2nd International Conference on Networking, Information Systems & Security" celebrado en Rabat, Marruecos. El comité organizador le otorgó el premio al 2do mejor artículo del evento.

Algunos esquemas de compartición de secretos recientes, con detección de trampas y que están basados en el esquema de A. Shamir, utilizan una técnica de descomposición para mejorar la eficiencia de la evaluación de una función verificadora. Como consecuencia esto permite una detección de trampas más eficiente. En el trabajo a presentar mostramos un breve análisis de los posibles valores de la función verificadora para algunos esquemas propuestos recientemente y resaltamos algunas consideraciones que deben ser tomadas en cuenta para nuevas propuestas. Además, proponemos un esquema que utiliza una técnica de descomposición sobre el anillo $\mathbb{Z}_{2^m}$ que permite una implementación más eficiente de la función verificadora y por tanto una detección de trampas más eficiente en la mayoría de los casos.

22. Matemáticas y Computación de *Blockchain*

Rafael Espinosa-García
(espinosa@cinvestav.mx)
SEES/Sistemas VLSI, Departamento de Ingeniería Eléctrica, Cinvestav-IPN
Ciudad de México
(Trabajo conjunto con Guillermo Morales-Luna[12])

Blockchain, conocida por su uso en *Bitcoin*, tiene potencial de transformar industrias enteras, como banca, seguros e Internet de las cosas (IoT). *Blockchain*, de Satoshi Nakamoto como*Bitcoin*, se ha modificado para superar ciertos problemas y hacerla más escalable y más asequible para reguladores. *Bitcoin* como sistema de pago se ha adaptado a nuevas formas de comunicación, y ha sido una moneda rápida, segura y sin fronteras [1]. Todo dinero digital completamente viable (o cualquier activo digital como acciones, bonos o licencias) conlleva dos problemas: la confirmación de la autenticidad y el problema del doble gasto. En una red de igual a igual en una arquitectura distribuida, los participantes comparten recursos [4], los que son necesarios para servicios de compartición de archivos, almacenes o espacios de colaboración, o bien para accederlos directamente. Contrario al sistema bancario, las transacciones de *Bitcoin*, son transmitidas, grabadas y almacenadas por los muchos participantes de la red y no en ningún servidor central, y se finalizan en minutos porque no se necesita ninguna conciliación. A diferencia de los activos físicos, el efectivo u otros activos digitales son archivos binarios, que pueden ser copiados. Si no hay intermediarios que mantengan un libro de contabilidad de saldos del titular de una cuenta, se podría reenviarlo y reutilizarlo. Esto es el *problema de doble gasto*. Cada "billete digital" debe verificarse en un libro de contabilidad central [2]. Por lo tanto, se requiere un registro autorizado de todas las transacciones del activo digital. La solución de Nakamoto para tratar ambos problemas se basa en un sistema de contabilidad constantemente actualizado y distribuido públicamente combinado con criptografía de clave pública (PKI) y un mecanismo de consenso [3]. Es importante conocer cómo opera el mecanismo de *blockchain*. En la conferencia presentaremos el fundamento matemático del sistema (por ejemplo, DSA con curvas elípticas y procesos numéricos principales), su forma de operación en la red y un caso de estudio en el área financiera.

Referencias

[1] Antonopoulos MA (2014) Mastering Bitcoin—unlocking digital currencies. O'Reilly.

[2] Cham D (1992) Achieving electronic privacy. Scientific American, 267(2):96–101

[3] Nakamoto S (2009) A peer-to-peer electronic cash system. `https://bitcoin.org/bitcoin.pdf`

[4] Schollmeier, Rüdiger. (2001). A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications. `http://tinyurl.com/RudigerPaper`

[12]Departamento de Computación, Cinvestav-IPN

23. Traffic database generation based on TCP scanning techniques for the analysis of the behaviour of a network scan

González Rodríguez Florencio Javier
Gómez Martínez María Teresa
González Flores Byron
Pacheco Rodríguez Hugo Sebastian
(fjavier_gonzalez@cic.ipn.mx, mtgomez@cic.ipn.mx, huropacheco@esimez.mx)

Centro de Investigación en Computación
México, D.F

Within a methodology for security evaluations, there exists a stage of identification where it is possible to get features from a target. On the other hand, the defensive side has the intention to detect and avoid such offensive techniques through the use of security controls like IDS, IPS, hardening, protocol scrubbers, and others. This research tries to improve reactive security controls, identifying whether a target is being scanned through the analysis of the behavior the traffic based on neural networks. The main contribution will be the implementation of the most common network architectures and the generation of traffic where TCP scanning techniques are executed to train the neural networks.

The Transmission Control Protocol (TCP) was designed as a highly reliable host-to-host protocol between hosts in packet-switched computer communication networks, and interconnected systems of such networks. When establishing communication between machines, it is necessary to use a format for this connection. This research takes advantage of TCP flow through the analysis of the packet's sequence during a connection. The TCP/IP fields that we extracted are Source IP address, source port, destination port, SYN flag, ACK flag, and RST flag.

Artificial neural networks (ANN) are generally considered tools that can help analyze the effect of the cause in complex systems within a big data framework. A neural network tool is capable of handling small data sets of experimental or observational data. Can help to identify the main causal factors that lead to changes in some variable that summarizes the behavior of a complex system. For example, in the security area, a scanner can be detected using a neural network due exist a common flow in connections.

Referencias

[1] Karen Scarfone, Murugiah Souppaya, Amanda Cody, Angela Orebaugh, Technical Guide to Information Security Testing and Assessment, U.S Department of Commerce, 2008.

24. CLIC-ODB: Cell Level Integrity and Completeness for Outsourced Database

Bruno Ramos Cruz
(brunoramos@inaoep.mx)

Coordinación de Ciencias Computacionales, INAOE
72840, Puebla, Puebla
(Trabajo conjunto con Lil María Rodríguez Henríquez[13], Saúl E. Pomares Hernández[14])

El cómputo en la nube es un modelo que ofrece servicios externalizados, uno de éstos son las bases de datos como servicio (DaaS) donde el cliente delega sus datos a un servidor para obtener ahorros en la administración del sistema, en recursos humanos, licencias de software, etcétera. Sin embargo, este nuevo paradigma también conlleva riesgos de seguridad que deben ser atendidos.

Existen principalmente tres preocupaciones que el propietario de los datos debe considerar: la confidencialidad, la integridad y la disponibilidad. Estas inquietudes han sido estudiadas por la comunidad criptográfica de manera independiente [1, 2, 3, 4, 5] debido a la complejidad que implican.

Específicamente la integridad en datos estructurados considera el escenario donde el servidor al que se le delega la base de datos no es confiable. Por lo que el cliente después de ejecutar una consulta, puede obtener como respuesta el conjunto de registros que satisfacen la consulta (respuesta *correcta*) o bien algún resultado *incorrecto*. Una respuesta *incorrecta* puede contener tuplas modificadas de forma no autorizada o incluir tuplas que no fueron delegadas por el cliente (comprometiendo la integridad), omitir tuplas que cumplen con las condiciones de la consulta (violentando la completitud) o incluir tuplas que existieron en alguna versión de la base de datos pero que no corresponden a la actual (comprometiendo la frescura). Por ello debe existir un proceso que pueda proteger al cliente de comportamientos maliciosos del servidor, tal proceso es conocido en la literatura como procesamiento de consultas autenticado.

El procesamiento de consultas autenticado considera otros aspectos entre los que destacan la granularidad, es decir a qué nivel de detalle (base de datos, tabla, fila o celda) se garantizará la integridad y los tipos de consulta que serán soportados (selección, rango, agragación, *joins*, etc). Estos aspectos imponen restricciones que hacen difícil proponer un esquema lo suficientemente robusto para soportar todas las posibles transacciones.

En este trabajo se propone un esquema criptográfico para el procesamiento de consultas autenticado con granularidad a nivel de celda que permite verificar integridad y completitud en consultas de selección y rango en bases de datos en la nube. El esquema propuesto emplea una estructura de datos probabilística conocida como filtro de Cuckoo para brindar integridad. Para garantizar la completitud utiliza otra estructura de datos llamada Bitmaps y una primitiva criptográfica conocida como códigos de autenticación de mensajes (MACs).

Referencias

[1] Boldyreva A., Chenette N., Lee Y., O Neill A. (2009) Order-Preserving Symmetric Encryption. In: Joux A. (eds) Advances in Cryptology - EUROCRYPT 2009. EUROCRYPT 2009. Lecture Notes in Computer Science, vol 5479. Springer, Berlin, Heidelberg.

[13]CONACyT-INAOE
[14]INAOE

[2] Etemad M., Küpçü A.(2019) Verifiable database outsourcing supporting join. Journal of Network and Computer Applications, vol 115.

[3] Ferretti L., Marchetti M., Andreolini M., Colajanni M. (2018) A symmetric cryptographic scheme for data integrity verification in cloud databases. Information Sciences, vol 422.

[4] Rodríguez-Henríquez L.M., Chakraborty D. (2013) RDAS: A Symmetric Key Scheme for Authenticated Query Processing in Outsourced Databases. In: Accorsi R., Ranise S. (eds) Security and Trust Management. STM 2013. Lecture Notes in Computer Science, vol 8203. Springer, Berlin, Heidelberg.

[5] Rodríguez-Henríquez L. M., Chakraborty D. (2014) Using bitmaps for executing range queries in encrypted databases. 11th International Conference on Security and Cryptography (SECRYPT), Vienna, 2014, pp. 1-7.

25. Firmas digitales estandarizadas y candidatos poscuánticos

José Rodríguez-Escobar
(luis.dominguez@cimat.mx)

Centro de Investigación en Matemáticas, A.C.
Zacatecas, Zacatecas
(Trabajo conjunto con Luis J. Dominguez Perez[15])

Las firmas digitales hoy en día son uno de los esquemas criptográficos más utilizados en internet, no solamente para fines de autenticación, en muchos países se tiene poder legar para firmar documentos electrónicamente. Es por este poder legal que debemos de investigar y desarrollar nuevas maneras, más rápidas y seguras, para proteger la información que queremos firmar.

Las firmas digitales proveen de algoritmos matemáticos para verificar que mensajes o documentos son genuinos. Para que una firma digital se pueda considerar confiable, debe de satisfacer tres condiciones: debe de proveer de autenticación para las partes, el signatario no puede decir que no firmó un documento (no-repudiación) y el mensaje debe de conservar su integridad, esto es, que no se altere en tránsito o en almacenamiento.

Los esquemas de firmas digitales cubren tres categorías, dos de ellas pertenecen a la Teoría de Números, y se componen de problemas clásicos: factorización de enteros y el problema del logaritmo discreto (en sus diversas variantes), la otra categoría se compone de los candidatos al concurso de estandarización de primitivas poscuánticas del NIST, y están basadas en problemas de retículas, polinomios de multivariables, funciones hash y otros. Actualmente el concurso NIST se encuentra en etapas avanzadas.

Actualmente, los estándares de firmas electrónicas se basan en las primeras dos categorías mencionadas: la firma RSA, la cual está basada en la dificultad de factorizar números sumamente grandes; y en las firmas tipo DSA, las cuales están basadas en la dificultad del problema del logaritmo discreto, que en este caso también presentan una variante basada en curvas elípticas.

Para el caso de las instituciones internacionales de estandarización, existen varios estándares en criptografía para las firmas digitales. En el caso de la IETF, se tiene el PKCS#1 versión 1.5 y actualmente la su versión v2.2, que hace referencia a la versión anteriormente mencionada.

[15] Centro de Investigación en Matemáticas

En el caso del IEEE se tiene el estándar IEEE1363-2000, IEEE 1363a-2004, IEEE 1363.1-2008, IEEE 1363.2-2008 y el IEEE 1363.3-201. Y para el caso del NIST, se tiene el Digital Signature Standard (DSS) 186-4 de 2013. Existen otros organismos que también estableces estándares; sin embargo, son de cobro.

En este trabajo de investigación analizamos los estándares de firmas digitales y analizamos las tendencias hacia el futuro. Presentaremos una discusión de los estándares, así como de tiempos de ejecución de las primitivas utilizando OpenSSL y otras herramientas disponibles.

Referencias

[1] Referencia: https://github.com/josscimat/OpenSSL_Implementations

26. Códigos abelianos minimales y sus extrañas dimensiones

Elias Javier Garcia Claro

(eliasjaviergarcia@gmail.com)

Universidad Autónoma Metropolitana,
Ciudad de México, CDMX

Resumen: Un código abeliano es un ideal de $\mathbb{F}_q[G]$. Se dice que un código abeliano es minimal si no contiene ningún ideal (salvo a si mismo y el ideal 0). Los códigos abelianos minimales son importantes para entender la retícula de ideales de $\mathbb{F}_q[G]$ cuando q y $|G|$ son primos relativos. En este caso, todo ideal de $\mathbb{F}_q[G]$ puede escribirse como suma directa de códigos abelianos minimales. Un problema de interes en el estudio de códigos abelianos es el de encontrar fórmulas o maneras eficientes de calcular la dimensiones de los códigos abelianos minimales. Existe una relación entre estas dimensiones y las cardinalidades de ciertas clases de equivalencia de G llamadas clases q-ciclotómicas. Vamos a explicar esta relación, y construir un método que se vasa en esta para calcular las dimensiones (módulo $Char(\mathbb{F}_q)$) de los códigos abelianos minimales en $\mathbb{F}_q[G]$.

Referencias

[1] C. Curtis, I. Reiner. Representation Theory of Finite Groups and Associative Algebras. Jhon Wiley and sons, 1962.

[2] C. Curtis, I. Reiner. Methods of representation theory with applications to finite groups and orders. vol. 1, John Wiley and sons, 1981.

[3] C. Ding, D. R. Kohel, S. Ling, Split group codes. IEEE Transactions on Information Theory 46 (2)(2000), 485-495.

[4] C. Polcino Milies and S. K. Sehgal, An Introduction to Group Rings, Kluwer academic publishers, 2002.

27. Usando paralelismo en el protocolo SIDH

Daniel Cervantes-Vázquez
(dcervantes@computacion.cs.cinvestav.mx / di.cervantesv@gmail.com)
Cinvestav - Departamento de computación
Ciudad de México
(Trabajo conjunto con José Eduardo-Ochoa-Jiménez y Francisco Rodríguez-Henriquez)

En la actualidad, la preocupación ante la creación de computadoras cuánticas poderosas ha ido en aumento debido a que en caso de existir, el internet como lo conocemos estaría desprotegido. La principal amenaza que trean consigo dichas computadoras es la posible implementación del algoritmo de Shor con el cuál, si se cuenta con recursos suficientes, es posible resolver el problema del logaritmo discreto y la factorización entera en tiempo polinomial. Con base en ésta posible amenaza el Instituto Nacional de Estándares y Tecnologías, NIST por sus siglas en inglés, lanzó un concurso para buscar protocolos criptográficos para intercambiar llaves y realizar firmas digitales, capaces de resistir el ataque de una computadora cuántica conocidos actualmente como protocolos post-cuánticos. Actuálmente el concurso va en la segunda ronda y uno de los candidatos que pasaron a ésta es el protocolo de Diffie-Hellman supersingular[1], SIDH por sus siglas en inglés, cuya seguridad descansa en el siguiente problema: dadas dos curvas elípticas supersingulares, es difífil encontrar una isogenia en particular entre ellas.

La principal ventaja del protocolo SIDH recae en la utilización de llaves cortas, en comparación con otros protocolos post-cuánticos como los basados en retículas o los basados en polinomios de varias variables. Por otro lado, el protocolo SIDH require una mayor cantidad de cómputos en comparación con los ya mencionados por lo que es necesario realizar optimizaciones tanto algorítmicas como aquellas que se aprovechan del hardware disponible. En éste trabajo presentamos una versión del protocolo SIDH que obtiene una aceleración considerable si se cuentan con al menos, dos núcleos disponibles para el cómputo del protocolo. Dicha versión es una versión a la que llamamos Diffie-Hellman supersingular extendido, eSIDH por sus siglas en inglés, por el hecho de que usamos enteros de la forma $p = 2^{e_2}3^{e_3}5^{e_5}f - 1$, a diferencia de los enteros usados en el protocolo SIDH que son de la forma $p = 2^{e_2}3^{e_3}f - 1$, donde en ambos casos, f es un entero pequeño tal que garantiza que p sea un número primo. Usar ésta clase de primos nos permite aprovechar el cómputo paralelo y, en algunos casos, encontrar primos con propiedades que ayuden a la reducción modular. Terminamos mostrando un caso más de como aprovechar el hardware disponible al utilizarlo en el recorrido de las estrategias utilizadas para computar las isogenias de cada participante[1].

Referencias

[1] *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies.* Luca De Feo and David Jao and Jérôme Plût. Cryptology ePrint Archive, Report 2011/506. 2011. https://eprint.iacr.org/2011/506

28. Códigos LCD asociados a ondeletas (wavelets)

Horacio Tapia-Recillas
(htr@xanum.uam.mx)
Universidad Autónoma Metropolitana-Iztapalapa, CDMX

Las transformadas de ondeletas (wavelet transform) particularmente de Haar y Daubechies, definidas sobre los números reales, tienen una variada gama de aplicación que cubren, entre otras: eliminación de ruido de imágenes y audio, compresión de señales y huellas digitales, reconocimiento de voz. Transformadas de ondeletas se han definido sobre campos finitos y usado para construir sistemas de cifrados en cascada y determinar códigos lineales de peso par. Recientemente los códigos LCD, Linearly Complementary Codes, han llamado la atención de varios grupos de trabajo por diversas razones que incluyen aplicaciones a seguridad informatíca. En esta plática se introduciran las transformadas de Haar y Daubechies sobre campos primos $\mathbb{Z}_p$ para ciertos valores del primo p, y se determinaraán códigos LCD.

29. Un protocolo seguro de comunicacioń I2I en redes vehiculares, basado en un esquema de secreto compartido

Juan Josué Gómez Olvera
(josueg@inaoep.mx)
Instituto Nacional de Astrofísica, Óptica y Electrónica
San Andrés Cholula, Puebla
(Lil María Xibai Rodríguez Henríquez [16], Saúl Eduardo Pomares Hernández [17])

Las redes vehiculares (VANET por sus siglas en inglés), es un paradigma que parte de la idea de dotar a vehículos con sensores, capacidades de procesamiento y de transmisión inalámbrica, de manera que les permita comunicarse e interactuar entre ellos. A este entorno se integra la infraestructura de las calles, cuya función es intercambiar información de interés que contribuya al sistema de transporte y la seguridad vial.

En el contexto de estas redes, han surgido nuevos servicios y aplicaciones esenciales para el desarrollo de sistemas de transporte inteligente. En el cual, la infraestructura vial desempeña un papel importante para proporcionar asistencia vial al conductor, contribuir al monitoreo del tráfico y a la eficiencia del transporte, entre otros.

Por otra parte, evitar el abuso de estos servicios por entidades maliciosas es crucial para el éxito de los mismos. Por ejemplo, el monitoreo de tráfico busca establecer mecanismos de auto-regularización de los semáforos inteligentes, si éstos se ven comprometidos, podría derivar en caos vial que paralice una ciudad, ocasione accidentes automovilísticos e inclusive la pérdida

[16] CONACyT-INAOE C.P. 72840, San Andrés Cholula, Puebla

[17] INAOE C.P. 72840, San Andrés Cholula, Puebla

de vidas humanas.

Por lo tanto en este tipo de aplicaciones se debe garantizar servicios de seguridad como la confidencialidad, autenticación, integridad, anonimato, entre otros. Específicamente en el caso de la confidencialidad en comunicaciones infraestructura a infraestructura I2I, diversos trabajos han sido propuestos suponiendo la existencia de infraestructura de llave pública (PKI por sus siglas en inglés) [1, 2]. Sin embargo, el hecho de que las VANET sean redes ad-hoc y sin infraestructura dificulta la existencia de entidades de confianza, requisito fundamental para este tipo de soluciones. Existen otras características de las VANETs que deben ser consideradas, entre las que destacan las restricciones espacio-temporales de la información, el desorden y pérdida de paquetes de datos, además del envío y la naturaleza asíncrona de la red.

En este trabajo se propone un protocolo de comunicación en grupo para la infraestructura vial, el cual respeta las restricciones espacio-temporales de la información y las características de la red. Este protocolo de comunicación se basa en un esquema de secreto compartido [3, 4], cuyo objetivo es proporcionar el servicio de confidencialidad.

Referencias

[1] Klaus Plobl, Hannes Federrath, A privacy aware and efficient security infrastructure for vehicular ad hoc networks, Computer Standards & Interfaces, Volume 30, Issue 6, 2008, Pages 390-397, ISSN 0920-5489.

[2] Neng-Wen Wang, Yueh-Min Huang, Wei-Ming Chen, A novel secure communication scheme in vehicular ad hoc networks, Computer Communications, Volume 31, Issue 12, 2008, Pages 2827-2837, ISSN 0140-3664.

[3] Abhishek Parakh, Subhash Kak, Space efficient secret sharing for implicit data security, Information Sciences, Volume 181, Issue 2, 2011, Pages 335-341, ISSN 0020-0255.

[4] L. Harn, "Group Authenticationïn IEEE Transactions on Computers, vol. 62, no. 9, pp. 1893-1898, Sept. 2013.

30. Nociones de Seguridad para Sistemas Blockchain

Víctor Gabriel Reyes Macedo
(vreyesm1102@alumno.ipn.mx)

Instituto Politécnico Nacional
07738 Gustavo A. Madero, Ciudad de México
(Trabajo conjunto con Gina Gallegos García[18]y Moisés Salinas Rosales[18])

Con la aparición de Bitcoin, surgió la tecnología de *cadena de bloques*, mejor conocida como *blockchain*, la cual se define como una red de intercambio y almacenamiento de datos, descentralizada y auditable, basada en protocolos criptográficos [1]. Esta tecnología ha encontrado, a lo largo de los años, un número creciente de aplicaciones en diversos campos de la actividad humana, desde el sector financiero, actividades gubernamentales, servicios de salud y logística, entre otros.

La ciencia detrás de la tecnología *blockchain* es la criptografía, mediante la cual se garantiza la integridad de la información que resguarda. Sin embargo, dependiendo de la aplicación, puede ser necesario garantizar, adicionalmente, propiedades como la privacidad y el anonimato de los usuarios. Un ejemplo de ello son las transacciones con criptomonedas, donde los usuarios no desean ser identificados por motivos de seguridad.

Por lo anterior, es importante contar con herramientas para evaluar el nivel de seguridad de los esquemas criptográficos; una de ellas es la *seguridad demostrable*, introducida por Goldwasser y Micali en [2], como un método con base en suposiciones de complejidad y un modelo de adversario. De acuerdo con Degabriele y Paterson [3], este método introduce definiciones formales de *seguridad* en la criptografía, y adopta técnicas de la probabilidad y la teoría de la complejidad computacional para analizar las construcciones criptográficas.

En esta ponencia, se presenta una introducción al uso de técnicas de seguridad demostrable, para la evaluación de la seguridad de sistemas basados *blockchain*. En particular, se abordan las transacciones con criptomonedas, por lo que se discutirán las nociones de seguridad que deben ser garantizadas, así como los modelos de seguridad en términos de dichas nociones y de las capacidades de un adversario [4].

Referencias

[1] Halpin, H., & Piekarska, M. (2017, April). Introduction to Security and Privacy on the Blockchain. In 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 1-3). IEEE.

[2] Goldwasser, S., & Micali, S. (1984). Probabilistic encryption. Journal of computer and system sciences, 28(2), 270-299.

[3] Degabriele, J. P., Paterson, K., & Watson, G. (2011). Provable security in the real world. IEEE Security & Privacy, 9(3), 33-41.

[4] Santiago, S. D., Garcia, G. G., Henriquez, L. M. R., & Cortes, N. C. (2016). A Brief Introduction to Provable Security. IEEE Latin America Transactions, 14(5), 2323-2332.

[18]Instituto Politécnico Nacional