Breve recuento histórico de la criptografía en México

Francisco Rodrǵuez-Henríquez
Departamento de Computación
CINVESTAV-IPN

13 de noviembre de 2020

Resumen

En esta charla, se presenta una selección panorámica de resultados criptográficos emblemáticos ocurridos en México durante los últimos cien años, incluyendo:

0. Una carta cortesiana
1. La carta robada
2. El Telegrama de Zimmermann
3. Quebrantamiento de un estándar de la IEEE para almacenamiento de bloques grandes
4. La obtención de un récord mundial para el quebrantamiento de ciertas instancias del problema del logaritmo discreto usando la súper computadora Abacus
5. Desarrollo de una Aplicación móvil para el rastreo de contactos COVID-19
6. Resultados novedosos en criptografía post-cuántica

Los últimos cuatro resultados reseñados corresponden a proyectos de criptografía y de seguridad informática desarrollados en el seno del Departamento de Computación en el transcurso de los últimos diez años.

Biografía

Francisco Rodríguez-Henríquez obtuvo el grado de doctor en junio del 2000 en el departamento de ingeniería eléctrica y computación de la Universidad Oregon State en Estados Unidos. De julio de 2000 a mayo de 2002 el doctor Rodríguez-Henríquez trabajó en compañías de seguridad informáticas de Estados Unidos y Alemania. A partir de mayo del 2002, el Dr. Rodríguez-Henríquez colabora con el Departamento de Computación del CINVESTAV-IPN en la ciudad de México, donde actualmente es profesor titular 3-D. Es co-autor de más de 80 artículos técnicos y capítulos de libro. Asimismo, él es el primer autor del libro: *"Cryptographic Algorithms on Reconfigurable Hardware"*, publicado por Springer en noviembre del 2006. El Dr. Rodríguez-Henríquez es miembro de la Academia Mexicana de Ciencias y ha sido o es miembro del comité editorial de las revistas *"Journal of Universal Computer Science"* de la Universidad de Graz, Austria, *"Journal of Cryptographic Engineering"* de Springer, *"the VLSI journal"* de Elsevier, *IEEE Transactions on emerging topics in computing* e *"IEEE Transactions on Computers"*.

Sus principales áreas de investigación son criptografía, aritmética computacional y seguridad informática. En su grupo de investigación, junto a sus tesistas de posgrado y colaboradores internacionales, el doctor Rodríguez-Henríquez ha obtenido varios récords de velocidad en implementaciones de algoritmos criptográficos basados en curvas elípticas, así como el récord mundial del quebramiento del logaritmo discreto para campos finitos de característica pequeña, el cual fue calculado utilizando la súper computadora Abacus del Cinvestav en julio del 2016. El Dr. Rodríguez-Henríquez es co-

fundador de la conferencia internacional en criptología y seguridad de la información (Latincrypt) y de la Escuela Avanzada de Criptología (ASCrypto), cuyas primeras ediciones fueron celebradas en Puebla en 2010 y en Sao Paulo en 2011, respectivamente. Desde entonces, Latincrypt y ASCrypto han sido organizadas en varias ciudades de Chile, Brasil, México y Cuba.

El doctor Rodríguez-Henríquez ha sido co-autor en diez ocasiones diferentes de artículos de investigación publicados en *"IEEE Transactions on Computers"*, la revista decana de computación de la IEEE.