SUMMER SCHOOL ON Cryptography

Crypto-CO 2 EDITION

June 10-14 2019
Medellín, Colombia

CONTACT INFORMATION

Daniel Cabarcas
John B. Baena

-Área Curricular en Matemáticas
-Facultad de Ciencias
-Tel.: (57-4) 430 93 22
Conmutador: (57-4) 430 90 00 Ext. 493 22
-E-mail: posmat_med@unal.edu.co
-Oficina: 43-105
-Universidad Nacional de Colombia
Sede Medellín

Valérie Gauthier

-Departamento de Matemáticas Aplicadas y Ciencias de la Computación - MACC
-Facultad de Ciencias Naturales y Matemáticas
-Universidad del Rosario
-Carrera 6 # 12 C - 16, oficina 502
-E-mail: macc@urosario.edu.co
Bogotá, Colombia
http://www.urosario.edu.co/Departamento-Macc/Inicio/

Martín Ochoa

-Cyxtera Technologies, Bogotá
-Bogotá, Colombia
-E-mail: martin.ochoa@cyxtera.com

Jointly organized with 17th International Conference on Applied Cryptography and Network Security (http://www.acns19.com/) which takes place the week before in Bogotá, Colombia.

Medellín, Colombia, June 10 – 14 (2019) (http://ciencias.medellin.unal.edu.co/eventos/cryptoco/)

SPONSOR

Fellows Colombia ICETEX

ruta n MEDELLÍN

ORGANIZED BY

Cyxtera

Universidad del Rosario

UNIVERSIDAD NACIONAL DE COLOMBIA

INVITED SPEAKERS

Daniel Bernstein

Ph.D. from University of California at Berkeley, and currently Professor at the Technische Universiteit Eindhoven, and a Research Professor of Computer Science at the University of Illinois at Chicago. Professor Bernstein is well known for his prolific research career, with important contributions to secure email and DNS services, stream ciphers, elliptic curves, coding theory, internet protocols, among others. He is also known for suing the United States Government in 1995 (Bernstein v. United States), challenging restrictions on the export of cryptography from the United States.

Francisco Rodríguez

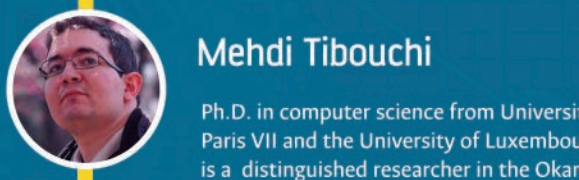
Ph.D. in Electrical and Computer Engineering from Oregon State Uni versity, and currently a research professor at Departamento de Computación CINVESTAV-IPN, México. His research areas are public and symmetric key cryptography, computer arithmetic, finite fields, algorithm implementation in reconfigurable hardware, information security and mobile computing. Professor Rodríguez has developed a variety of cores that implement cryptographic algorithms and finite-field arithmetic algorithms in reconfigurable hardware platforms.

Jintai Ding

Ph.D. in mathematics from Yale University, currently Professor at the University of Cincinnati and adjunct professor at several universities in other countries. Professor Ding's research areas are Information Security, Computational Algebra, Classical Cryptography, Postquantum Cryptography, Hardware implementation, Number Theory, Representation Theory, and Mathematical Physics. He is the principal submitter of two of the proposals in the NIST postquantum competition. Professor Ding is also recognized for his famous key exchange protocol based on LWE.

WHAT IS CRYPTO-CO?

Crypto-CO is a summer school in Cryptology, the mathematical foundation of information security, and it was held for the first time in Bogotá in 2016. We will have international lecturers with long research trajectories in the area. During the week-long school, they will give introductory lectures on current trends in Cryptology. Crypto-CO aims to consolidate a community around the topics of Cryptology and applications to security that involves academia, government and industry.



Mehdi Tibouchi

Ph.D. in computer science from University Paris VII and the University of Luxembourg. He is a distinguished researcher in the Okamoto Research Laboratory, at the NTT Secure Platform Laboratories in Tokyo, Japan. His research focuses on public-key cryptology, including various mathematical aspects of algebraic curve cryptography, RSA cryptanalysis, and provable protocol constructions. He was a Ph.D. candidate under David Naccache and Jean-Sébastien Coron, working in the Crypto Team of the ENS Computer Science Lab.

Tanja Lange

Ph.D. from Universität Duisburg-Essen, Germany, and currently chair of the Coding Theory and Cryptology group at the Technische Universiteit Eindhoven, scientific director of the Eindhoven Institute for the Protection of Systems and Information, and one of the coordinators of PQCRYPTO, a European research consortium that has been charged with the development of postquantum cryptography. Professor Lange performs research in theoretical and applied areas of coding theory and cryptology. She is also interested in elliptic curve, hyperelliptic curve and postquantum cryptography.