LatinCrypt 2014
Florianópolis, 17-19 September

Program

LabSEC nic.br egi.br

Núcleo de Informação e Coordenação do Ponto BR

Comitê Gestor da Internet no Brasil

CNPQ
CAPES

FAPESC

UNIVERSIDADE FEDERAL DE SANTA CATARINA

Carleton UNIVERSITY

ine CTC • UFSC

INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH

Program Overview

	Wed 17	Thr 18	Fri 19
08:50 - 09:00	Opening Remarks by Alfred Menezes, Diego Aranha, Daniel Panario, Ricardo Custódio		
09:00 - 10:30	Session 1: Cryptographic Engineering I	Session 3: Cryptographic Engineering II	Session 5: Attacks
10:30 - 11:00	Coffee Break	Coffee break	
11:00 - 11:30	Invited Talk How cryptography is used and fails in the real world J. Alex Halderman (University of Michigan, USA)	Invited Talk ML confidential machine learning on encrypted data Kristin Lauter (Microsoft Research, USA)	Coffee break
11:30 - 12:00			Invited Talk Impact of intelligence agency activities on research and practice in cryptography Jacob Appelbaum (The Tor Project, Germany)
12:00 - 12:30	Lunch	Lunch	
12:30 - 14:00			Lunch
14:00 - 15:30	Session 2: Side Channel Attacks and Countermeasures	Session 4: Privacy	Session 6: Cryptographic Protocols
15:30 - 16:00	Invited Talk A critical review of Privacy Technologies Claudia Diaz (Katholieke Universiteit Leuven, Belgium)	Coffee break	Coffee break
16:00 - 16:30		Student session 1: Students & Pos-docs	Student session 2: Students & Pos-docs
16:30 - 18:00	Welcome Coquetail		
18:00 - 18:30		Free time	Free time
18:00 - 21:00	Free time		
21:00 - 23:30		Gala dinner	

Latincrypt 2014 - P r o g r a m

Wednesday, September 17th

08:00 - 18:00	Registration	
08:50 - 09:00	Opening Remarks by Alfred Menezes, Diego Aranha, Daniel Panario, and Ricardo Custódio	
09:00 - 10:30	**Session 1: Cryptographic Engineering I**	
	09:00 - 09:30	Full Size High Security ECC Implementation on MSP430 Microcontrollers **Gesine Hinterwälder, Amir Moradi, Michael Hutter, Peter Schwabe, Christof Paar** (Ruhr-University Bochum, Ruhr-University Bochum, TU Graz, Radboud University Nijmegen, Ruhr-University Bochum)
	09:30 - 10:00	Efficient Integer Encoding for Homomorphic Encryption via Ring Isomorphisms **Matthias Geihs, Daniel Cabarcas** (TU Darmstadt, Universidad Nacional de Colombia)
	10:00 - 10:30	Analysis of NORX **Jean-Philippe Aumasson, Philipp Jovanovic, Samuel Neves** (Kudelski Security, University of Passau, University of Coimbra)
10:30 - 11:00	Coffee break	
11:00 - 12:00	Invited Talk	How cryptography is used and fails in the real world **J. Alex Halderman** (University of Michigan, USA)
12:00 - 14:00	Lunch	
14:00 - 15:30	**Session 2: Side Channel Attacks and Countermeasures**	
	14:00 - 14:30	Efficient Leakage-Resilient Pseudorandom Functions from Hard-to-Invert Leakages **Fabrizio De Santis, Stefan Rass** (Technische Universitaet Muenchen, Alpen-Adria Universitaet)
	14:30 - 15:00	RSA and Elliptic Curve Least Significant Bit Security **Dionathan Nakamura, Routo Terada** (University of Sao Paulo)
	15:00 - 15:30	Isogeny volcanoes of elliptic curves and Sylow subgroups **Mireille Fouquet, Josep M. Miret, Javier Valera** (Université Paris Diderot, Universitat de Lleida, Universitat de Lleida)
15:30 - 16:30	Invited Talk	A critical review of Privacy Technologies **Claudia Diaz** (Katholieke Universiteit Leuven, Belgium)
16:30 - 18:30	**Welcome Cocktail**	

Latincrypt 2014 - P r o g r a m

Thursday, September 18th

08:00 - 18:00	Registration	
09:00 - 10:30	**Session 3: Cryptographic Engineering II**	
	09:00 - 09:30	TweetNaCl: A crypto library in 100 tweets **Daniel J. Bernstein, Bernard van Gastel, Wesley Janssen, Tanja Lange, Peter Schwabe, Sjaak Smetsers** (University of Illinois at Chicago, Eindhoven University of Technology; Radboud University Nijmegen, Radboud University Nijmegen, Eindhoven University of Technology, Radboud University Nijmegen, Radboud University Nijmegen)
	09:30 - 10:00	High-speed signatures from standard lattices **Özgür Dagdelen, Rachid El Bansarkhani, Florian Göpfert, Tim Güneysu, Tobias Oder, Thomas Pöppelmann, Ana Helena Sánchez, Peter Schwabe** (TU Darmstadt, TU Darmstadt, TU Darmstadt, Ruhr-University Bochum, Ruhr-University Bochum, Ruhr-University Bochum, Radboud University Nijmegen, Radboud University Nijmegen)
	10:00 - 10:30	Block Cipher Speed and Energy Efficiency Records on the MSP430 -- System Design Tradeoffs for 16-bit Embedded Applications **Benjamin Buhrow, Paul Riemer, Mike Shea, Barry Gilbert, Erik Daniel** (Mayo Clinic)
10:30 - 11:00	Coffee break	
11:00 - 12:00	Invited Talk	ML confidential machine learning on encrypted data **Kristin Lauter** (Microsoft Research, USA)
12:00 - 14:00	Lunch	
14:00 - 15:30	**Session 4: Privacy**	
	14:00 - 14:30	Beating the Birthday Paradox in Dining Cryptographer Networks **Pablo Garcia, Jeroen van de Graaf, Alejandro Hevia, Alfredo Viola** (Universidad Nacional de San Luis, Universidade Federal de Minas Gerais, Universidad de Chile, Universidad de la Republica)
	14:30 - 15:00	Private Asymmetric Fingerprinting: a Protocol with Optimal Traitor Tracing using Tardos Codes **Caroline Fontaine, Sébastien Gambs, Julien Lolive, Cristina Onete** (Télécom Bretagne/CNRS/Lab-STICC, Université de Rennes 1 - Inria, Télécom Bretagne - Inria, Université de Rennes 1)
	15:00 - 15:30	Anonymous Authentication with Shared Secrets **Joel Alwen, Martin Hirt, Ueli Maurer, Arpita Patra, Pavel Raykov** (ETH Zurich, ETH Zurich, ETH Zurich, ISI Kolkata, India, ETH Zurich)
15:30 - 16:00	**Coffee break**	

Latincrypt 2014 - P r o g r a m

Thursday, September 18th

08:00 - 18:00	Registration	
15:30 - 16:00	Coffee break	
16:00 - 18:00	**Student Session 1: Students & Pos-docs**	
	16:00 - 16:15	Deniability, Undeniability and Signatures **Alonso González Ulloa** (Departamento de Ciencias de la Computación, Universidad de Chile)
	16:15 - 16:30	PUF+PAKE = Mutual multifactor authentication for secure banking **Amanda Cristina Davi Resende** Department of Computer Science – UnB
	16:30 - 16:45	An efficient software implementation of XMSS **Ana Karina D. S. de Oliveira** FACOM – University of Mato Grosso do Sul
	16:45 - 17:00	Recovering of Integer Equivalent from wt-NAF Expansion **Armando Faz Hernández** Institute of Computing, University of Campinas
	17:00 - 17:15	Parallel Improved Schnorr-Euchner Enumeration for High-Performance CVP and SVP Computation **Artur Mariano** Institute for Scientific Computing, Darmstadt University of Technology
	17:15 - 17:30	Discrete authorization and efficient mutual authentication in capacity sharing-enabled networks **Cassius de Oliveira Puodzius** Escola Politécnica - University of São Paulo (USP)
	17:30 - 17:45	Faster Point Doubling on Twisted Hessian Curves **Chitchanok Chuengsatiansup** Eindhoven University of Technology, The Netherlands
	17:45 - 18:00	Results on the Application of Visual Cryptography for Products and Online Transactions Authentication **Franz Pietz** Institute of Computing - University of Campinas
18:00 - 21:30	Free time	
21:30 - 23:30	**Gala Dinner**	

Latincrypt 2014 - P r o g r a m

Friday, September 19th

08:00 - 18:00	Registration	
09:00 - 11:00	**Session 5: Attacks**	
	09:00 - 09:30	On Key Recovery Attacks against Existing Somewhat Homomorphic Encryption Schemes **Massimo Chenal, Qiang Tang** (University of Luxembourg)
	09:30 - 10:00	Practical attacks on AES-like cryptographic hash functions **Stefan Kölbl, Christian Rechberger** (Technical University of Denmark)
	10:00 - 10:30	Key Recovery Attacks on Recent Authenticated Ciphers **Andrey Bogdanov, Christoph Dobraunig, Maria Eichlseder, Martin M. Lauridsen, Florian Mendel, Martin Schläffer, Elmar Tischhauser** (Technical University of Denmark, TU Graz, TU Graz, Technical University of Denmark, TU Graz, TU Graz, Technical University of Denmark)
	10:30 - 11:00	Tuning GaussSieve for Speed **Robert Fitzpatrick, Christian Bischof, Johannes Buchmann, Özgür Dagdelen, Florian Göpfert, Artur Mariano, Bo-Yin Yang** (Academia Sinica, TU Darmstadt, TU Darmstadt, TU Darmstadt, TU Darmstadt, TU Darmstadt, Academia Sinica)
11:00 - 11:30	Coffee break	
11:30 - 12:30	Invited Talk	Impact of intelligence agency activities on research and practice in cryptography **Jacob Appelbaum** (The Tor Project, Germany)
12:30 - 14:00	Lunch	
14:00 - 15:30	**Session 6: Cryptographic Protocols**	
	14:00 - 14:30	Efficient Distributed Tag-Based Encryption and its Application to Group Signatures with Efficient Distributed Traceability **Essam Ghadafi** (University of Bristol)
	14:30 - 15:00	How to Leak a Secret and Reap the Rewards too **Vishal Saraswat, Sumit Kumar Pandey** (CRRao AIMSCS, Indian Statistical Institute)
	15:00 - 15:30	Extending Oblivious Transfer Efficiently, or - How to get active security with constant cryptographic overhead **Enrique Larraia** (University of Bristol)
15:30 - 16:00	**Coffee break**	

Latincrypt 2014 - P r o g r a m

Friday, September 19th

08:00 - 18:00	Registration	
15:30 - 16:00	Coffee break	
16:00 - 18:00	**Student Session 2: Students & Pos-docs**	
	16:00 - 16:15	A Two-Level Evaluation of R-Ate and Optimal Ate Pairings over Barreto-Naehrig Elliptic Curves **Leandro Aparecido Sangalli** (University of Campinas)
	16:15 - 16:30	Software implementation of SHA-3 using AVX2 **Roberto Cabral** (Institute of Computing, University of Campinas)
	16:30 - 16:45	Polynomials for GLS binary curves at 192- and 256-bit security levels **Thomaz Oliveira** (Computer Science Department, CINVESTAV-IPN)
	16:45 - 17:00	Locating modifications in signed data **Thaís Bardini Idalino** (University of Santa Catarina - UFSC)
	17:00 - 17:15	Algebraic Attack Implementation against Multivariate Quadratic Cryptosystems **Juan Grados** (Laboratório Nacional de Computação Científica - LNCC)
	17:15 - 17:30	Solving large sparse linear systems over finite fields using GPUs **Luis Rivera-Zamarripa** (Centro de Investigación en Computación, IPN)
	17:30 - 17:45	ARM Implementation of two-factor authentication protocols **José Eduardo Ochoa Jiménez** (Computer Science Department, CINVESTAV-IPN)
	17:45 - 18:00	Lyra2: a password hashing schemes with tunable memory and processing costs **Ewerton R. Andrade** (Escola Politécnica – University of São Paulo)
18:00 -	**Good bye**	