Students and Posdocs Accepted Speakers LatinCrypt 2014

Deniability, Undeniability and Signatures
Alonso González Ulloa
Departamento de Ciencias de la Computación, Universidad de Chile

PUF+PAKE = Mutual multifactor authentication for secure banking
Amanda Cristina Davi Resende
Department of Computer Science – UnB

An efficient software implementation of XMSS
Ana Karina D. S. de Oliveira
FACOM – UFMS

Recovering of Integer Equivalent from wt-NAF Expansion
Armando Faz Hernández
Institute of Computing, University of Campinas.

Parallel Improved Schnorr-Euchner Enumeration for High-Performance CVP and SVP Computation
Artur Mariano
Institute for Scientific Computing, Darmstadt University of Technology

Discrete authorization and efficient mutual authentication in capacity sharing-enabled networks
Cassius de Oliveira Puodzius
Escola Politécnica da USP - Universidade de São Paulo (USP)

Faster Point Doubling on Twisted Hessian Curves
Chitchanok Chuengsatiansup
Eindhoven University of Technology, The Netherlands

Lyra2: A hash scheme for passwords with fitting memory and processing costs
Ewerton R. Andrade
Escola Politécnica – Universidade de São Paulo

Results on the Application of Visual Cryptography for Products and Online Transactions Authentication
Franz Pietz
Institute of Computing - University of Campinas

A Two-Level Evaluation of R-Ate and Optimal Ate Pairings over Barreto-Naehrig Elliptic Curves
Leandro Aparecido Sangalli
State University of Campinas

Software implementation of SHA-3 using AVX2
Roberto Cabral
Institute of Computing, University of Campinas

Polynomials for GLS binary curves at 192- and 256-bit security levels
Thomaz Oliveira
Computer Science Department, CINVESTAV-IPN

Locating modifications in signed data
Thaís Bardini Idalino
Universidade Federal de Santa Catarina

Algebraic Attack Implementation against Multivariate Quadratic Cryptosystems
Juan Grados
Laboratório Nacional de Computação Científica (LNCC)

Solving large sparse linear systems over finite fields using GPUs
Luis Rivera-Zamarripa
Centro de Investigación en Computación, IPN

ARM Implementation of two-factor authentication protocols
José Eduardo Ochoa Jiménez
Computer Science Department, CINVESTAV-IPN