Accepted Papers LatinCrypt 2014

On Key Recovery Attacks against Existing Somewhat Homomorphic Encryption Schemes
Massimo Chenal, Qiang Tang
(University of Luxembourg)

Efficient Integer Encoding for Homomorphic Encryption via Ring Isomorphisms
Matthias Geihs, Daniel Cabarcas
(Technische Universität Darmstadt, Universidad Nacional de Colombia)

Efficient Distributed Tag-Based Encryption and its Application to Group Signatures with Efficient Distributed Traceability
Essam Ghadafi
(University of Bristol)

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)

How to Leak a Secret and Reap the Rewards too
Vishal Saraswat, Sumit Kumar Pandey
(CRRao AIMSCS, Indian Statistical Institute)

Analysis of NORX
Jean-Philippe Aumasson, Philipp Jovanovic, Samuel Neves
(Kudelski Security, University of Passau, University of Coimbra)

Extending Oblivious Transfer Efficiently, or - How to get active security with constant cryptographic overhead
Enrique Larraia
(University of Bristol)

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)

Practical attacks on AES-like cryptographic hash functions
Stefan Kölbl, Christian Rechberger
(Technical University of Denmark)

Efficient Leakage-Resilient Pseudorandom Functions from Hard-to-Invert Leakages
Fabrizio De Santis, Stefan Rass
(Technische Universitaet Muenchen, Alpen-Adria Universitaet)

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)

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)

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)

RSA and Elliptic Curve Least Significant Bit Security *
Dionathan Nakamura, Routo Terada
(University of Sao Paulo)

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)

Isogeny volcanoes of elliptic curves and Sylow subgroups *
Mireille Fouquet, Josep M. Miret, Javier Valera
(Université Paris Diderot, Universitat de Lleida, Universitat de Lleida)

PIMENTO: Privacy-preservIng asyMmetric fingErpriNting protocol based on 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)

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)

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)