## Contents

### Invited Talks

Private Computation on Encrypted Genomic Data ......................... 3  
*Kristin Lauter, Adriana López-Alt, and Michael Naehrig*

### Cryptographic Engineering

Full-Size High-Security ECC Implementation on MSP430 Microcontrollers . . . 31  
*Gesine Hinterwälder, Amir Moradi, Michael Hutter, Peter Schwabe, and Christof Paar*

Efficient Integer Encoding for Homomorphic Encryption via Ring Isomorphisms ................................................................. 48  
*Mattias Geihs and Daniel Cabarcas*

TweetNaCl: A Crypto Library in 100 Tweets ............................... 64  
*Daniel J. Bernstein, Bernard van Gastel, Wesley Janssen, Tanja Lange, Peter Schwabe, and Sjaak Smetsers*

High-Speed Signatures from Standard Lattices .......................... 84  
*Özgür Dagdelen, Rachid El Bansarkhani, Florian Göpfert, Tim Güneysu, Tobias Oder, Thomas Pöppelmann, Ana Helena Sánchez, and Peter Schwabe*

Block Cipher Speed and Energy Efficiency Records on the MSP430: System Design Trade-Offs for 16-Bit Embedded Applications ................. 104  
*Benjamin Buhrow, Paul Riemer, Mike Shea, Barry Gilbert, and Erik Daniel*

### Side-Channel Attacks and Countermeasures

On Efficient Leakage-Resilient Pseudorandom Functions with Hard-to-Invert Leakages ................................................................. 127  
*Fabrizio De Santis and Stefan Rass*

RSA and Elliptic Curve Least Significant Bit Security .................. 146  
*Dionathan Nakamura and Routo Terada*

Isogeny Volcanoes of Elliptic Curves and Sylow Subgroups ........... 162  
*Mireille Fouquet, Josep M. Miret, and Javier Valera*
Privacy

Beating the Birthday Paradox in Dining Cryptographer Networks
Pablo García, Jeroen van de Graaf, Alejandro Hevia, and Alfredo Viola
179

Private Asymmetric Fingerprinting: A Protocol with Optimal Traitor Tracing Using Tardos Codes
Caroline Fontaine, Sébastien Gambs, Julien Lolive, and Cristina Onete
199

Anonymous Authentication with Shared Secrets
Joël Alwen, Martin Hirt, Ueli Maurer, Arpita Patra, and Pavel Raykov
219

Cryptanalysis

On Key Recovery Attacks Against Existing Somewhat Homomorphic Encryption Schemes
Massimo Chenal and Qiang Tang
239

Practical Attacks on AES-like Cryptographic Hash Functions
Stefan Kölbl and Christian Rechberger
259

Key Recovery Attacks on Recent Authenticated Ciphers
Andrey Bogdanov, Christoph Dobraunig, Maria Eichlseder, Martin M. Lauridsen, Florian Mendel, Martin Schläffer, and Elmar Tischhauser
274

Tuning GaussSieve for Speed
Robert Fitzpatrick, Christian Bischof, Johannes Buchmann, Özgür Dagdelen, Florian Göpfert, Artur Mariano, and Bo-Yin Yang
288

Analysis of NORX: Investigating Differential and Rotational Properties
Jean-Philippe Aumasson, Philipp Jovanovic, and Samuel Neves
306

Cryptographic Protocols

Efficient Distributed Tag-Based Encryption and Its Application to Group Signatures with Efficient Distributed Traceability
Essam Ghadafi
327

How to Leak a Secret and Reap the Rewards Too
Vishal Saraswat and Sumit Kumar Pandey
348

Extending Oblivious Transfer Efficiently: or - How to Get Active Security with Constant Cryptographic Overhead
Enrique Larraia
368

Author Index
387
Progress in Cryptology - LATINCRYPT 2014
Third International Conference on Cryptology and
Information Security in Latin America Florianópolis,
Brazil, September 17-19, 2014 Revised Selected Papers
Aranha, D.F.; Menezes, A. (Eds.)
2015, XII, 387 p. 64 illus., Softcover
ISBN: 978-3-319-16294-2