

# Contents

## Invited Talks

Private Computation on Encrypted Genomic Data . . . . .	3
<i>Kristin Lauter, Adriana López-Alt, and Michael Naehrig</i>	

## Cryptographic Engineering

Full-Size High-Security ECC Implementation on MSP430 Microcontrollers . . .	31
<i>Gesine Hinterwälder, Amir Moradi, Michael Hutter, Peter Schwabe, and Christof Paar</i>	
Efficient Integer Encoding for Homomorphic Encryption via Ring Isomorphisms . . . . .	48
<i>Matthias Geihs and Daniel Cabarcas</i>	
TweetNaCl: A Crypto Library in 100 Tweets . . . . .	64
<i>Daniel J. Bernstein, Bernard van Gastel, Wesley Janssen, Tanja Lange, Peter Schwabe, and Sjaak Smetsers</i>	
High-Speed Signatures from Standard Lattices . . . . .	84
<i>Özgür Dagdelen, Rachid El Bansarkhani, Florian Göpfert, Tim Güneysu, Tobias Oder, Thomas Pöppelmann, Ana Helena Sánchez, and Peter Schwabe</i>	
Block Cipher Speed and Energy Efficiency Records on the MSP430: System Design Trade-Offs for 16-Bit Embedded Applications . . . . .	104
<i>Benjamin Buhrow, Paul Riemer, Mike Shea, Barry Gilbert, and Erik Daniel</i>	

## Side-Channel Attacks and Countermeasures

On Efficient Leakage-Resilient Pseudorandom Functions with Hard-to-Invert Leakages . . . . .	127
<i>Fabrizio De Santis and Stefan Rass</i>	
RSA and Elliptic Curve Least Significant Bit Security . . . . .	146
<i>Dionathan Nakamura and Routo Terada</i>	
Isogeny Volcanoes of Elliptic Curves and Sylow Subgroups. . . . .	162
<i>Mireille Fouquet, Josep M. Miret, and Javier Valera</i>	

**Privacy**

Beating the Birthday Paradox in Dining Cryptographer Networks . . . . .	179
<i>Pablo García, Jeroen van de Graaf, Alejandro Hevia, and Alfredo Viola</i>	
Private Asymmetric Fingerprinting: A Protocol with Optimal Traitor Tracing Using Tardos Codes . . . . .	199
<i>Caroline Fontaine, Sébastien Gambs, Julien Lolive, and Cristina Onete</i>	
Anonymous Authentication with Shared Secrets . . . . .	219
<i>Joël Alwen, Martin Hirt, Ueli Maurer, Arpita Patra, and Pavel Raykov</i>	

**Cryptanalysis**

On Key Recovery Attacks Against Existing Somewhat Homomorphic Encryption Schemes . . . . .	239
<i>Massimo Chenal and Qiang Tang</i>	
Practical Attacks on AES-like Cryptographic Hash Functions . . . . .	259
<i>Stefan Kölbl and Christian Rechberger</i>	
Key Recovery Attacks on Recent Authenticated Ciphers . . . . .	274
<i>Andrey Bogdanov, Christoph Dobraunig, Maria Eichlseder, Martin M. Lauridsen, Florian Mendel, Martin Schläffer, and Elmar Tischhauser</i>	
Tuning GaussSieve for Speed . . . . .	288
<i>Robert Fitzpatrick, Christian Bischof, Johannes Buchmann, Özgür Dagdelen, Florian Göpfert, Artur Mariano, and Bo-Yin Yang</i>	
Analysis of NORX: Investigating Differential and Rotational Properties. . . . .	306
<i>Jean-Philippe Aumasson, Philipp Jovanovic, and Samuel Neves</i>	

**Cryptographic Protocols**

Efficient Distributed Tag-Based Encryption and Its Application to Group Signatures with Efficient Distributed Traceability . . . . .	327
<i>Essam Ghadafi</i>	
How to Leak a Secret and Reap the Rewards Too. . . . .	348
<i>Vishal Saraswat and Sumit Kumar Pandey</i>	
Extending Oblivious Transfer Efficiently: or - How to Get Active Security with Constant Cryptographic Overhead . . . . .	368
<i>Enrique Larraia</i>	
<b>Author Index</b> . . . . .	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