

Kristin Lauter · Francisco Rodríguez-Henríquez (Eds.)

Progress in Cryptology – LATINCRYPT 2015

4th International Conference on Cryptology
and Information Security in Latin America
Guadalajara, Mexico, August 23–26, 2015
Proceedings

Contents

Cryptographic Protocols

Efficient RKA-Secure KEM and IBE Schemes Against Invertible Functions	3
<i>Eiichiro Fujisaki and Keita Xagawa</i>	
Simulation-Based Secure Functional Encryption in the Random Oracle Model	21
<i>Vincenzo Iovino and Karol Żebroski</i>	
The Simplest Protocol for Oblivious Transfer	40
<i>Tung Chou and Claudio Orlandi</i>	

Foundations

Depth Optimized Efficient Homomorphic Sorting	61
<i>Gizem S. Çetin, Yarkin Doröz, Berk Sunar, and Erkey Savaş</i>	
The Chain Rule for HILL Pseudoentropy, Revisited	81
<i>Krzysztof Pietrzak and Maciej Skórski</i>	

Post-Quantum Cryptography

Faster Sieving for Shortest Lattice Vectors Using Spherical Locality-Sensitive Hashing	101
<i>Thijs Laarhoven and Benne de Weger</i>	
FHEW with Efficient Multibit Bootstrapping	119
<i>Jean-François Biasse and Luis Ruiz</i>	

Symmetric Key Cryptanalysis

Improved Top-Down Techniques in Differential Cryptanalysis	139
<i>Itai Dinur, Orr Dunkelman, Masha Gutman, and Adi Shamir</i>	
Algebraic Analysis of the Simon Block Cipher Family	157
<i>Håvard Raddum</i>	
Cryptanalysis of the Full 8.5-Round REESSE3+ Block Cipher	170
<i>Jorge Nakahara Jr.</i>	

Meet-in-the-Middle Attacks on Reduced-Round Hierocrypt-3	187
<i>Ahmed Abdelkhalek, Riham AlTawy, Mohamed Tolba, and Amr M. Youssef</i>	
State-Recovery Analysis of Spritz	204
<i>Ralph Ankele, Stefan Kölbl, and Christian Rechberger</i>	
We Still Love Pairings	
Computing Optimal 2-3 Chains for Pairings	225
<i>Alex Capuñay and Nicolas Thériault</i>	
Subgroup Security in Pairing-Based Cryptography.	245
<i>Paulo S.L.M. Barreto, Craig Costello, Rafael Misoczki, Michael Naehrig, Geovandro C.C.F. Pereira, and Gustavo Zanon</i>	
Curves in Cryptography	
Twisted Hessian Curves.	269
<i>Daniel J. Bernstein, Chitchanok Chuengsatiansup, David Kohel, and Tanja Lange</i>	
Improved Sieving on Algebraic Curves	295
<i>Vanessa Vitse and Alexandre Wallet</i>	
Attacking a Binary GLS Elliptic Curve with Magma	308
<i>Jesús-Javier Chi and Thomaz Oliveira</i>	
Cryptographic Engineering	
Fast Implementation of Curve25519 Using AVX2.	329
<i>Armando Faz-Hernández and Julio López</i>	
High-Performance Ideal Lattice-Based Cryptography on 8-Bit ATxmega Microcontrollers	346
<i>Thomas Pöppelmann, Tobias Oder, and Tim Güneysu</i>	
An Efficient Software Implementation of the Hash-Based Signature Scheme MSS and Its Variants	366
<i>Ana Karina D.S. de Oliveira and Julio López</i>	
Author Index	385