## Contents

### Lattices

Efficient (Ideal) Lattice Sieving Using Cross-Polytope LSH .......................... 3  
*Anja Becker and Thijs Laarhoven*

On the Hardness of LWE with Binary Error: Revisiting the Hybrid  
Lattice-Reduction and Meet-in-the-Middle Attack ................................. 24  
*Johannes Buchmann, Florian Göpfert, Rachel Player,*  
*and Thomas Wunderer*

An Efficient Lattice-Based Signature Scheme with Provably  
Secure Instantiation ........................................ 44  
*Sedat Akleylek, Nina Bindel, Johannes Buchmann, Juliane Krämer,*  
*and Giorgia Azzurra Marson*

### Elliptic Curves

A Fast and Compact FPGA Implementation of Elliptic Curve Cryptography  
Using Lambda Coordinates ........................................ 63  
*Burak Gövem, Kimmo Järvinen, Kris Aerts, Ingrid Verbauwhede,*  
*and Nele Mentens*

Three Dimensional Montgomery Ladder, Differential Point Tripling  
on Montgomery Curves and Point Quintupling on Weierstrass’  
and Edwards Curves ............................................. 84  
*Srinivasa Rao Subramanya Rao*

### Secret-Key Cryptanalysis

Cryptanalysis of PRINCE with Minimal Data ........................................ 109  
*Shahram Rasoolzadeh and Håvard Raddum*

Authentication Key Recovery on Galois/Counter Mode (GCM) .................. 127  
*John Mattsson and Magnus Westerlund*

### Efficient Implementations

Extreme Pipelining Towards the Best Area-Performance Trade-Off  
in Hardware ...................................................... 147  
*Stjepan Picek, Dominik Sisejkovic, Domagoj Jakobovic, Lejla Batina,*  
*Bohan Yang, Danilo Sijacic, and Nele Mentens*
A Deeper Understanding of the XOR Count Distribution in the Context of Lightweight Cryptography .................................................. 167
   Sumanta Sarkar and Siang Meng Sim

Secure Protocols

Prover-Efficient Commit-and-Prove Zero-Knowledge SNARKs. .............. 185
   Helger Lipmaa

On the Security of the (F)MQV Protocol. ..................................... 207
   Augustin P. Sarr and Philippe Elbaz-Vincent

Non-Interactive Verifiable Secret Sharing for Monotone Circuits.......... 225
   Ge Bai, Ivan Damgård, Claudio Orlandi, and Yu Xia

Fast Oblivious AES A Dedicated Application of the MiniMac Protocol ... 245
   Ivan Damgård and Rasmus Zakarias

Certificate Validation in Secure Computation and Its Use in Verifiable Linear Programming ......................................................... 265
   Sebastiaan de Hoogh, Berry Schoenmakers, and Meilof Veeningen

Software-Only Two-Factor Authentication Secure Against Active Servers ... 285
   Julien Bringer, Hervé Chabanne, and Roch Lescuyer

Public-Key Cryptography

Attribute-Based Fully Homomorphic Encryption with a Bounded Number of Inputs ................................................................. 307
   Michael Clear and Ciarán McGoldrick

Adaptively Secure Unrestricted Attribute-Based Encryption with Subset Difference Revocation in Bilinear Groups of Prime Order ............ 325
   Pratish Datta, Ratna Dutta, and Sourav Mukhopadhyay

Weak Keys for the Quasi-Cyclic MDPC Public Key Encryption Scheme ... 346
   Magali Bardet, Vlad Dragoi, Jean-Gabriel Luque, and Ayoub Otmani

Author Index ................................................................................. 369
Progress in Cryptology – AFRICACRYPT 2016
8th International Conference on Cryptology in Africa,
Fes, Morocco, April 13-15, 2016, Proceedings
Pointcheval, D.; Nitaj, A.; Rachidi, T. (Eds.)
2016, X, 369 p. 49 illus., Softcover
ISBN: 978-3-319-31516-4