

Contents

Lattices

Efficient (Ideal) Lattice Sieving Using Cross-Polytope LSH	3
<i>Anja Becker and Thijs Laarhoven</i>	
On the Hardness of LWE with Binary Error: Revisiting the Hybrid Lattice-Reduction and Meet-in-the-Middle Attack	24
<i>Johannes Buchmann, Florian Göpfert, Rachel Player, and Thomas Wunderer</i>	
An Efficient Lattice-Based Signature Scheme with Provably Secure Instantiation	44
<i>Sedat Akleylek, Nina Bindel, Johannes Buchmann, Juliane Krämer, and Giorgia Azzurra Marson</i>	

Elliptic Curves

A Fast and Compact FPGA Implementation of Elliptic Curve Cryptography Using Lambda Coordinates	63
<i>Burak Gövem, Kimmo Järvinen, Kris Aerts, Ingrid Verbauwhede, and Nele Mentens</i>	
Three Dimensional Montgomery Ladder, Differential Point Tripling on Montgomery Curves and Point Quintupling on Weierstrass' and Edwards Curves	84
<i>Srinivasa Rao Subramanya Rao</i>	

Secret-Key Cryptanalysis

Cryptanalysis of PRINCE with Minimal Data	109
<i>Shahram Rasoolzadeh and Håvard Raddum</i>	
Authentication Key Recovery on Galois/Counter Mode (GCM).	127
<i>John Mattsson and Magnus Westerlund</i>	

Efficient Implementations

Extreme Pipelining Towards the Best Area-Performance Trade-Off in Hardware	147
<i>Stjepan Picek, Dominik Sisejkovic, Domagoj Jakobovic, Lejla Batina, Bohan Yang, Danilo Sijacic, and Nele Mentens</i>	

A Deeper Understanding of the XOR Count Distribution in the Context of Lightweight Cryptography	167
<i>Sumanta Sarkar and Siang Meng Sim</i>	

Secure Protocols

Prover-Efficient Commit-and-Prove Zero-Knowledge SNARKs.	185
<i>Helger Lipmaa</i>	
On the Security of the (F)HMQV Protocol.	207
<i>Augustin P. Sarr and Philippe Elbaz-Vincent</i>	
Non-Interactive Verifiable Secret Sharing for Monotone Circuits.	225
<i>Ge Bai, Ivan Damgård, Claudio Orlandi, and Yu Xia</i>	
Fast Oblivious AES A Dedicated Application of the MiniMac Protocol	245
<i>Ivan Damgård and Rasmus Zakarias</i>	
Certificate Validation in Secure Computation and Its Use in Verifiable Linear Programming	265
<i>Sebastiaan de Hoogh, Berry Schoenmakers, and Meilof Veeningen</i>	
Software-Only Two-Factor Authentication Secure Against Active Servers . . .	285
<i>Julien Bringer, Hervé Chabanne, and Roch Lescuyer</i>	

Public-Key Cryptography

Attribute-Based Fully Homomorphic Encryption with a Bounded Number of Inputs	307
<i>Michael Clear and Ciarán McGoldrick</i>	
Adaptively Secure Unrestricted Attribute-Based Encryption with Subset Difference Revocation in Bilinear Groups of Prime Order	325
<i>Pratish Datta, Ratna Dutta, and Sourav Mukhopadhyay</i>	
Weak Keys for the Quasi-Cyclic MDPC Public Key Encryption Scheme	346
<i>Magali Bardet, Vlad Dragoi, Jean-Gabriel Luque, and Ayoub Otmani</i>	

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