Table of Contents

New Results for Rank-Based Cryptography 1
Philippe Gaborit, Olivier Ruatta, Julien Schrek, and Gilles Zémor

Public-Key Cryptography

Proxy Re-Encryption Scheme Supporting a Selection of Delegatees 13
Julien Devigne, Eleonora Guerrini, and Fabien Laguillaumie

Trapdoor Privacy in Asymmetric Searchable Encryption Schemes 31
Afonso Arriaga, Qiang Tang, and Peter Ryan

Kurosawa-Desmedt Key Encapsulation Mechanism, Revisited 51
Kaoru Kurosawa and Le Trieu Phong

Hash Functions

Differential Biases in Reduced-Round Keccak 69
Sourav Das and Willi Meier

Practical Distinguishers against 6-Round Keccak-*f* Exploiting Self-Symmetry 88
Sukhendu Kuila, Dhiman Saha, Madhumangal Pal, and Dipanwita Roy Chowdhury

Preimage Attacks on Reduced-Round Stribog 109
Riham AlTawy and Amr M. Youssef

Secret-Key Cryptanalysis

Breaking the IOC Authenticated Encryption Mode 126
Paul Bottinelli, Reza Reyhanitabar, and Serge Vaudenay

New Treatment of the BSW Sampling and Its Applications to Stream Ciphers 136
Lin Ding, Chenhui Jin, Jie Guan, and Chuanda Qi

Multidimensional Zero-Correlation Linear Cryptanalysis of E2 147
Long Wen, Meiqin Wang, and Andrey Bogdanov

Public-Key Cryptanalysis and Number Theory

Further Improvement of Factoring RSA Moduli with Implicit Hint 165
Liqiang Peng, Lei Hu, Jun Xu, Zhangjie Huang, and Yonghong Xie

Progress in Cryptology ? AFRICACRYPT 2014
2014

digitalisiert durch
IDS Basel/Bern, im Auftrag der
Schweizerischen Nationalbibliothek

New Attacks on the RSA Cryptosystem 178
Abderrahmane Nitaj, Muhammad Rezal Kamel Ariffin, Dieaa I. Nassr, and Hatem M. Bahig

Formulae for Computation of Tate Pairing on Hyperelliptic Curve Using Hyperelliptic Nets 199
Christophe Tran

Hardware Implementation

New Speed Records for Montgomery Modular Multiplication on 8-bit AVR Microcontrollers 215
Zhe Liu and Johann Großschädl

Minimizing S-Boxes in Hardware by Utilizing Linear Transformations... 235
Sebastian Kutzner, Phuong Ha Nguyen, Axel Poschmann, and Marc Stöttinger

Efficient Masked S-Boxes Processing – A Step Forward – 251
Vincent Grosso, Emmanuel Prouff, and François-Xavier Standaert

A More Efficient AES Threshold Implementation 267
Begül Bilgin, Benedikt Gierlichs, Svetla Nikova, Ventzislav Nikov, and Vincent Rijmen

Protocols

Constant Rounds Almost Linear Complexity Multi-party Computation for Prefix Sum 285
Kazuma Ohara, Kazuo Ohta, Koutarou Suzuki, and Kazuki Yoneyama

Position-Based Cryptography from Noisy Channels 300
Stefan Dziembowski and Maciej Zdanowicz

Lattice-Based Cryptography

A Comparison of the Homomorphic Encryption Schemes FV and YASHE 318
Tancrède Lepoint and Michael Naehrig

Towards Lattice Based Aggregate Signatures 336
Rachid El Bansarkhani and Johannes Buchmann

Public-Key Cryptography

A Second Look at Fischlin's Transformation 356
Özgür Dagdelen and Daniele Venturi

Anonymous IBE from Quadratic Residuosity with Improved Performance 377
Michael Clear, Hitesh Tewari, and Ciarán McGoldrick

Expressive Attribute Based Signcryption with Constant-Size Ciphertext 398
Y. Sreenivasa Rao and Ratna Dutta

Secret-Key Cryptography

DRECON: DPA Resistant Encryption by Construction 420
Suvadeep Hajra, Chester Rebeiro, Shivam Bhasin, Gaurav Bajaj, Sahil Sharma, Sylvain Guilley, and Debdeep Mukhopadhyay

COUNTER-bDM: A Provably Secure Family of Multi-Block-Length Compression Functions 440
Farzaneh Abed, Christian Forler, Eik List, Stefan Lucks, and Jakob Wenzel

Universal Hash-Function Families: From Hashing to Authentication 459
Basel Alomair

Author Index 475