

Contents

Invited Talk

- The Realm of the Pairings 3
*Diego F. Aranha, Paulo S.L.M. Barreto, Patrick Longa,
and Jefferson E. Ricardini*

Lattices Part I

- A Three-Level Sieve Algorithm for the Shortest Vector Problem 29
Feng Zhang, Yanbin Pan, and Gengran Hu
- Improvement and Efficient Implementation of a Lattice-Based
Signature Scheme 48
Rachid El Bansarkhani and Johannes Buchmann
- Towards Practical Lattice-Based Public-Key Encryption on Reconfigurable
Hardware 68
Thomas Pöppelmann and Tim Güneysu

Invited Talk

- Practical Approaches to Varying Network Size in Combinatorial Key
Predistribution Schemes 89
Kevin Henry, Maura B. Paterson, and Douglas R. Stinson

Discrete Logarithms

- A Group Action on \mathbb{Z}_p^\times and the Generalized DLP with Auxiliary Inputs 121
Jung Hee Cheon, Taechan Kim, and Yong Soo Song
- Solving a 6120-bit DLP on a Desktop Computer 136
Faruk Göloğlu, Robert Granger, Gary McGuire, and Jens Zumbrägel

Stream Ciphers and Authenticated Encryption

- How to Recover Any Byte of Plaintext on RC4 155
Toshihiro Ohigashi, Takanori Isobe, Yuhei Watanabe, and Masakatu Morii
- The LOCAL Attack: Cryptanalysis of the Authenticated Encryption
Scheme ALE 174
Dmitry Khovratovich and Christian Rechberger

AEGIS: A Fast Authenticated Encryption Algorithm. 185
Hongjun Wu and Bart Preneel

Post-quantum (Hash-Based and System Solving)

Fast Exhaustive Search for Quadratic Systems in \mathbb{F}_2 on FPGAs 205
Charles Bouillaguet, Chen-Mou Cheng, Tung Chou, Ruben Niederhagen, and Bo-Yin Yang

Faster Hash-Based Signatures with Bounded Leakage 223
Thomas Eisenbarth, Ingo von Maurich, and Xin Ye

White Box Crypto

White-Box Security Notions for Symmetric Encryption Schemes 247
Cécile Delerablée, Tancrede Lepoint, Pascal Paillier, and Matthieu Rivain

Two Attacks on a White-Box AES Implementation 265
Tancrede Lepoint, Matthieu Rivain, Yoni De Mulder, Peter Roelse, and Bart Preneel

Block Ciphers

Extended Generalized Feistel Networks Using Matrix Representation 289
Thierry P. Berger, Marine Minier, and Gaël Thomas

Zero-Correlation Linear Cryptanalysis with FFT and Improved Attacks on ISO Standards Camellia and CLEFIA. 306
Andrey Bogdanov, Huizheng Geng, Meiqin Wang, Long Wen, and Baudoin Collard

Implementing Lightweight Block Ciphers on $\times 86$ Architectures 324
Ryad Benadjila, Jian Guo, Victor Lomné, and Thomas Peyrin

Invited Talk

A New Index Calculus Algorithm with Complexity $L(1/4 + o(1))$ in Small Characteristic 355
Antoine Joux

Lattices Part II

High Precision Discrete Gaussian Sampling on FPGAs 383
Sujoy Sinha Roy, Frederik Vercauteren, and Ingrid Verbauwhede

Discrete Ziggurat: A Time-Memory Trade-Off for Sampling
 from a Gaussian Distribution over the Integers. 402
*Johannes Buchmann, Daniel Cabarcas, Florian Göpfert,
 Andreas Hülsing, and Patrick Weiden*

Elliptic Curves, Pairings and RSA

A High-Speed Elliptic Curve Cryptographic Processor for Generic Curves
 over $GF(p)$ 421
Yuan Ma, Zongbin Liu, Wuqiong Pan, and Jiwu Jing

Exponentiating in Pairing Groups 438
Joppe W. Bos, Craig Costello, and Michael Naehrig

Faster Repeated Doublings on Binary Elliptic Curves 456
Christophe Doche and Daniel Sutantyo

Montgomery Multiplication Using Vector Instructions 471
*Joppe W. Bos, Peter L. Montgomery, Daniel Shumow,
 and Gregory M. Zaverucha*

Hash Functions and MACs

Improved Single-Key Distinguisher on HMAC-MD5 and Key Recovery
 Attacks on Sandwich-MAC-MD5 493
Yu Sasaki and Lei Wang

Provable Second Preimage Resistance Revisited. 513
Charles Boullaguet and Bastien Vayssière

Multiple Limited-Birthday Distinguishers and Applications 533
Jérémy Jean, María Naya-Plasencia, and Thomas Peyrin

Side-Channel Attacks

Horizontal Collision Correlation Attack on Elliptic Curves 553
Aurélie Bauer, Eliane Jaulmes, Emmanuel Prouff, and Justine Wild

When Reverse-Engineering Meets Side-Channel Analysis –
 Digital Lockpicking in Practice 571
*David Oswald, Daehyun Strobel, Falk Schellenberg, Timo Kasper,
 and Christof Paar*

Author Index 589



<http://www.springer.com/978-3-662-43413-0>

Selected Areas in Cryptography -- SAC 2013
20th International Conference, Burnaby, BC, Canada,
August 14-16, 2013, Revised Selected Papers
Lange, T.; Lauter, K.; Lisonek, P. (Eds.)
2014, XV, 590 p. 107 illus., Softcover
ISBN: 978-3-662-43413-0