

# Contents

## Invited Talk

The Realm of the Pairings . . . . .	3
<i>Diego F. Aranha, Paulo S.L.M. Barreto, Patrick Longa, and Jefferson E. Ricardini</i>	

## Lattices Part I

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

## Invited Talk

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

## Discrete Logarithms

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

## Stream Ciphers and Authenticated Encryption

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

AEGIS: A Fast Authenticated Encryption Algorithm. . . . .	185
<i>Hongjun Wu and Bart Preneel</i>	

**Post-quantum (Hash-Based and System Solving)**

Fast Exhaustive Search for Quadratic Systems in $\mathbb{F}_2$ on FPGAs . . . . .	205
<i>Charles Bouillaguet, Chen-Mou Cheng, Tung Chou, Ruben Niederhagen, and Bo-Yin Yang</i>	
Faster Hash-Based Signatures with Bounded Leakage . . . . .	223
<i>Thomas Eisenbarth, Ingo von Maurich, and Xin Ye</i>	

**White Box Crypto**

White-Box Security Notions for Symmetric Encryption Schemes . . . . .	247
<i>Cécile Delerablée, Tancrede Lepoint, Pascal Paillier, and Matthieu Rivain</i>	
Two Attacks on a White-Box AES Implementation . . . . .	265
<i>Tancrede Lepoint, Matthieu Rivain, Yoni De Mulder, Peter Roelse, and Bart Preneel</i>	

**Block Ciphers**

Extended Generalized Feistel Networks Using Matrix Representation . . . . .	289
<i>Thierry P. Berger, Marine Minier, and Gaël Thomas</i>	
Zero-Correlation Linear Cryptanalysis with FFT and Improved Attacks on ISO Standards Camellia and CLEFIA. . . . .	306
<i>Andrey Bogdanov, Huizheng Geng, Meiqin Wang, Long Wen, and Baudoin Collard</i>	
Implementing Lightweight Block Ciphers on $\times 86$ Architectures . . . . .	324
<i>Ryad Benadjila, Jian Guo, Victor Lomné, and Thomas Peyrin</i>	

**Invited Talk**

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

**Lattices Part II**

High Precision Discrete Gaussian Sampling on FPGAs . . . . .	383
<i>Sujoy Sinha Roy, Frederik Vercauteren, and Ingrid Verbauwhede</i>	

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

## Elliptic Curves, Pairings and RSA

A High-Speed Elliptic Curve Cryptographic Processor for Generic Curves over $\text{GF}(p)$ . . . . .	421
<i>Yuan Ma, Zongbin Liu, Wuqiong Pan, and Jiwu Jing</i>	
Exponentiating in Pairing Groups . . . . .	438
<i>Joppe W. Bos, Craig Costello, and Michael Naehrig</i>	
Faster Repeated Doublings on Binary Elliptic Curves . . . . .	456
<i>Christophe Doche and Daniel Sutanty</i>	
Montgomery Multiplication Using Vector Instructions . . . . .	471
<i>Joppe W. Bos, Peter L. Montgomery, Daniel Shumow, and Gregory M. Zaverucha</i>	

## Hash Functions and MACs

Improved Single-Key Distinguisher on HMAC-MD5 and Key Recovery Attacks on Sandwich-MAC-MD5 . . . . .	493
<i>Yu Sasaki and Lei Wang</i>	
Provable Second Preimage Resistance Revisited. . . . .	513
<i>Charles Bouillaguet and Bastien Vayssière</i>	
Multiple Limited-Birthday Distinguishers and Applications . . . . .	533
<i>Jérémy Jean, María Naya-Plasencia, and Thomas Peyrin</i>	

## Side-Channel Attacks

Horizontal Collision Correlation Attack on Elliptic Curves . . . . .	553
<i>Aurélien Bauer, Eliane Jaulmes, Emmanuel Prouff, and Justine Wild</i>	
When Reverse-Engineering Meets Side-Channel Analysis – Digital Lockpicking in Practice . . . . .	571
<i>David Oswald, Daehyun Strobel, Falk Schellenberg, Timo Kasper, and Christof Paar</i>	

Author Index . . . . .	589
------------------------	-----

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