

Contents

Malicious Hashing: Eve's Variant of SHA-1.	1
<i>Ange Albertini, Jean-Philippe Aumasson, Maria Eichlseder, Florian Mendel, and Martin Schl��ffer</i>	
Binary Elligator Squared	20
<i>Diego F. Aranha, Pierre-Alain Fouque, Chen Qian, Mehdi Tibouchi, and Jean-Christophe Zavalowicz</i>	
Batch NFS	38
<i>Daniel J. Bernstein and Tanja Lange</i>	
An Improvement of Linear Cryptanalysis with Addition Operations with Applications to FEAL-8X	59
<i>Eli Biham and Yaniv Carmeli</i>	
Colliding Keys for SC2000-256	77
<i>Alex Biryukov and Ivica Nikoli��</i>	
Faster Binary-Field Multiplication and Faster Binary-Field MACs	92
<i>Daniel J. Bernstein and Tung Chou</i>	
OMD: A Compression Function Mode of Operation for Authenticated Encryption	112
<i>Simon Cogliani, Diana-��tefania Maimu��, David Naccache, Rodrigo Portella do Canto, Reza Reyhanitabar, Serge Vaudenay, and Damian Viz��r</i>	
Security Amplification for the Composition of Block Ciphers: Simpler Proofs and New Results	129
<i>Beno��t Cogliati, Jacques Patarin, and Yannick Seurin</i>	
Improved Differential Cryptanalysis of Round-Reduced Speck	147
<i>Itai Dinur</i>	
Differential Cryptanalysis of SipHash	165
<i>Christoph Dobraunig, Florian Mendel, and Martin Schl��ffer</i>	
Weak Instances of PLWE	183
<i>Kirsten Eisentr��ger, Sean Hallgren, and Kristin Lauter</i>	
The Usage of Counter Revisited: Second-Preimage Attack on New Russian Standardized Hash Function	195
<i>Jian Guo, J��r��my Jean, Ga��tan Leurent, Thomas Peyrin, and Lei Wang</i>	

Side-Channel Analysis of Montgomery’s Representation Randomization	212
<i>Éliane Jaulmes, Emmanuel Prouff, and Justine Wild</i>	
Practical Cryptanalysis of PAES	228
<i>Jérémy Jean, Ivica Nikolić, Yu Sasaki, and Lei Wang</i>	
Diffusion Matrices from Algebraic-Geometry Codes with Efficient SIMD Implementation	243
<i>Daniel Augot, Pierre-Alain Fouque, and Pierre Karpman</i>	
Error-Tolerant Side-Channel Cube Attack Revisited.	261
<i>Zhenqi Li, Bin Zhang, Arnab Roy, and Junfeng Fan</i>	
A Generic Algorithm for Small Weight Discrete Logarithms in Composite Groups.	278
<i>Alexander May and Ilya Ozerov</i>	
Linear Biases in AEGIS Keystream.	290
<i>Brice Minaud</i>	
Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers	306
<i>Nicky Mouha, Bart Mennink, Anthony Van Herrewege, Dai Watanabe, Bart Preneel, and Ingrid Verbauwhede</i>	
Fast Point Multiplication Algorithms for Binary Elliptic Curves with and Without Precomputation	324
<i>Thomaz Oliveira, Diego F. Aranha, Julio López, and Francisco Rodríguez-Henríquez</i>	
Partial Key Exposure Attacks on RSA: Achieving the Boneh-Durfee Bound . . .	345
<i>Atsushi Takayasu and Noboru Kunihiro</i>	
Solving the Discrete Logarithm of a 113-bit Koblitz Curve with an FPGA Cluster	363
<i>Erich Wenger and Paul Wolfger</i>	
Author Index	381

Selected Areas in Cryptography -- SAC 2014
21st International Conference, Montreal, QC, Canada,
August 14-15, 2014, Revised Selected Papers
Joux, A.; Youssef, A. (Eds.)
2014, X, 381 p. 66 illus., Softcover
ISBN: 978-3-319-13050-7