Contents

Malicious Hashing: Eve’s Variant of SHA-1 ........................................ 1
Ange Albertini, Jean-Philippe Aumasson, Maria Eichlseder,
Florian Mendel, and Martin Schläffer

Binary Elligator Squared ......................................................... 20
Diego F. Aranha, Pierre-Alain Fouque, Chen Qian, Mehdi Tibouchi,
and Jean-Christophe Zapalowicz

Batch NFS ................................................................. 38
Daniel J. Bernstein and Tanja Lange

An Improvement of Linear Cryptanalysis with Addition Operations
with Applications to FEAL-8X ................................................. 59
Eli Biham and Yaniv Carmeli

Colliding Keys for SC2000-256 ................................................. 77
Alex Biryukov and Ivica Nikolić

Faster Binary-Field Multiplication and Faster Binary-Field MACs ............. 92
Daniel J. Bernstein and Tung Chou

OMD: A Compression Function Mode of Operation
for Authenticated Encryption .................................................. 112
Simon Cogliani, Diana-Ştefania Maimuţ, David Naccache,
Rodrigo Portella do Canto, Reza Reyhanitabar,
Serge Vaudenay, and Damian Vizár

Security Amplification for the Composition of Block Ciphers:
Simpler Proofs and New Results .............................................. 129
Benoit Cogliati, Jacques Patarin, and Yannick Seurin

Improved Differential Cryptanalysis of Round-Reduced Speck .................. 147
Itai Dinur

Differential Cryptanalysis of SipHash ........................................... 165
Christoph Do Braunig, Florian Mendel, and Martin Schläffer

Weak Instances of PLWE ..................................................... 183
Kirsten Eisenträger, Sean Hallgren, and Kristin Lauter

The Usage of Counter Revisited: Second-Preimage Attack
on New Russian Standardized Hash Function .................................. 195
Jian Guo, Jérémy Jean, Gaëtan Leurent, Thomas Peyrin, and Lei Wang
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Side-Channel Analysis of Montgomery’s Representation Randomization</td>
<td>212</td>
</tr>
<tr>
<td>Eliane Jaulmes, Emmanuel Prouff, and Justine Wild</td>
<td></td>
</tr>
<tr>
<td>Practical Cryptanalysis of PAES</td>
<td>228</td>
</tr>
<tr>
<td>Jérémy Jean, Ivica Nikolić, Yu Sasaki, and Lei Wang</td>
<td></td>
</tr>
<tr>
<td>Diffusion Matrices from Algebraic-Geometry Codes with Efficient</td>
<td>243</td>
</tr>
<tr>
<td>SIMD Implementation</td>
<td></td>
</tr>
<tr>
<td>Daniel Augot, Pierre-Alain Fouque, and Pierre Karpman</td>
<td></td>
</tr>
<tr>
<td>Error-Tolerant Side-Channel Cube Attack Revisited.</td>
<td>261</td>
</tr>
<tr>
<td>Zhenqi Li, Bin Zhang, Arnab Roy, and Junfeng Fan</td>
<td></td>
</tr>
<tr>
<td>A Generic Algorithm for Small Weight Discrete Logarithms in</td>
<td>278</td>
</tr>
<tr>
<td>Composite Groups</td>
<td></td>
</tr>
<tr>
<td>Alexander May and Ilya Ozerov</td>
<td></td>
</tr>
<tr>
<td>Linear Biases in AEGIS Keystream</td>
<td>290</td>
</tr>
<tr>
<td>Brice Minaud</td>
<td></td>
</tr>
<tr>
<td>Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers</td>
<td>306</td>
</tr>
<tr>
<td>Nicky Mouha, Bart Mennink, Anthony Van Herrewege, Dai Watanabe,</td>
<td></td>
</tr>
<tr>
<td>Bart Preneel, and Ingrid Verbauwhede</td>
<td></td>
</tr>
<tr>
<td>Fast Point Multiplication Algorithms for Binary Elliptic Curves</td>
<td>324</td>
</tr>
<tr>
<td>with and Without Precomputation</td>
<td></td>
</tr>
<tr>
<td>Thomaz Oliveira, Diego F. Aranha, Julio López,</td>
<td></td>
</tr>
<tr>
<td>and Francisco Rodríguez-Henríquez</td>
<td></td>
</tr>
<tr>
<td>Partial Key Exposure Attacks on RSA: Achieving the Boneh-Durfee Bound</td>
<td>345</td>
</tr>
<tr>
<td>Atsushi Takayasu and Noboru Kunihiro</td>
<td></td>
</tr>
<tr>
<td>Solving the Discrete Logarithm of a 113-bit Koblitz Curve</td>
<td>363</td>
</tr>
<tr>
<td>with an FPGA Cluster</td>
<td></td>
</tr>
<tr>
<td>Erich Wenger and Paul Wolfsger</td>
<td></td>
</tr>
<tr>
<td>Author Index</td>
<td>381</td>
</tr>
</tbody>
</table>
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