Table of Contents

Non-integral Asymmetric Functions

Efficient and Secure Algorithms for GLV-Based Scalar Multiplication and Their Implementation on GLV-GLS Curves .......... 1
Armando Faz-Hernández, Patrick Longa, and Ana H. Sánchez

An Improved Compression Technique for Signatures Based on Learning with Errors .......................................................... 28
Shi Bai and Steven D. Galbraith

Public-Key Encryption

A Generic View on Trace-and-Revoke Broadcast Encryption Schemes ... 48
Dennis Hofheinz and Christoph Striecks

Broadcast Steganography .......................................................... 64
Nelly Fazio, Antonio R. Nicolosi, and Irippuge Milinda Perera

Practical Dual-Receiver Encryption: Soundness, Complete Non-malleability, and Applications .............................. 85
Sherman S.M. Chow, Matthew Franklin, and Haibin Zhang

Hardware Implementations

Attacking PUF-Based Pattern Matching Key Generators via Helper Data Manipulation ...................................................... 106
Jeroen Delvaux and Ingrid Verbauwhede

On Increasing the Throughput of Stream Ciphers ...................... 132
Frederik Armknecht and Vasily Mikhalev

On Double Exponentiation for Securing RSA against Fault Analysis .... 152
Duc-Phong Le, Matthieu Rivain, and Chik How Tan

Side-Channel Attacks

On the Practical Security of a Leakage Resilient Masking Scheme ..... 169
Emmanuel Prouff, Matthieu Rivain, and Thomas Roche

The Myth of Generic DPA... and the Magic of Learning ............ 183
Carolyn Whitnall, Elisabeth Oswald, and François-Xavier Standaert
Hardware Implementation and Side-Channel Analysis of Lapin .................. 206
   Lubos Gaspar, Gaëtan Leurent, and François-Xavier Standaert

Symmetric Encryption and Cryptanalysis

Automatic Search for Differential Trails in ARX Ciphers ......................... 227
   Alex Biryukov and Vesselin Velichkov

CBEAM: Efficient Authenticated Encryption from Feebly One-Way $\phi$
Functions ................................................................. 251
   Markku-Juhani O. Saarinen

Beyond Modes: Building a Secure Record Protocol from a
Cryptographic Sponge Permutation ......................................... 270
   Markku-Juhani O. Saarinen

Digital Signatures

Group Signatures with Message-Dependent Opening in the Standard
Model ................................................................. 286
   Benoît Libert and Marc Joye

Practical Distributed Signatures in the Standard Model ......................... 307
   Yujue Wang, Duncan S. Wong, Qianhong Wu,
   Sherman S.M. Chow, Bo Qin, and Jianwei Liu

Decentralized Traceable Attribute-Based Signatures .......................... 327
   Ali El Kaafarani, Essam Ghadafi, and Dalia Khader

Protocols

Rethinking Verifiably Encrypted Signatures: A Gap in
Functionality and Potential Solutions ..................................... 349
   Theresa Calderon, Sarah Meiklejohn, Hovav Shacham, and
   Brent Waters

P$^2$OFE: Privacy-Preserving Optimistic Fair Exchange of Digital
Signatures ............................................................. 367
   Qiong Huang, Duncan S. Wong, and Willy Susilo

2-Pass Key Exchange Protocols from CPA-Secure KEM ....................... 385
   Kaoru Kurosawa and Jun Furukawa

Hash Function Cryptanalysis

Analysis of BLAKE2 ................................................................ 402
   Jian Guo, Pierre Karpman, Ivica Nikolić, Lei Wang, and Shuang Wu
<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>444</td>
<td>Practical Collision Attack on 40-Step RIPEMD-128</td>
<td>Gaoli Wang</td>
</tr>
<tr>
<td>461</td>
<td>Applications of Cryptographic Primitives</td>
<td></td>
</tr>
<tr>
<td>481</td>
<td>Key Wrapping with a Fixed Permutation</td>
<td>Dmitry Khovratovich</td>
</tr>
<tr>
<td>501</td>
<td>Author Index</td>
<td></td>
</tr>
</tbody>
</table>