

Contents

Block Ciphers

Complementing Feistel Ciphers	3
<i>Alex Biryukov and Ivica Nikolić</i>	
On the Wrong Key Randomisation and Key Equivalence Hypotheses in Matsui's Algorithm 2	19
<i>Andrey Bogdanov and Elmar Tischhauser</i>	
Cryptanalysis of WIDEA	39
<i>Gaëtan Leurent</i>	

Invited Talk

Towards Secure Distance Bounding	55
<i>Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay</i>	

Lightweight Block Ciphers

Reflection Cryptanalysis of PRINCE-Like Ciphers	71
<i>Hadi Soleimany, Céline Blondeau, Xiaoli Yu, Wenling Wu, Kaisa Nyberg, Huiling Zhang, Lei Zhang, and Yanfeng Wang</i>	
Security Analysis of PRINCE	92
<i>Jérémy Jean, Ivica Nikolić, Thomas Peyrin, Lei Wang, and Shuang Wu</i>	
Cryptanalysis of Round-Reduced LED.	112
<i>Ivica Nikolić, Lei Wang, and Shuang Wu</i>	

Tweakable Block Ciphers

Tweakable Blockciphers with Asymptotically Optimal Security	133
<i>Rodolphe Lampe and Yannick Seurin</i>	

Stream Ciphers I

Smashing WEP in a Passive Attack	155
<i>Pouyan Sepehrdad, Petr Sušil, Serge Vaudenay, and Martin Vuagnoux</i>	
Full Plaintext Recovery Attack on Broadcast RC4	179
<i>Takanori Isobe, Toshihiro Ohigashi, Yuhei Watanabe, and Masakatu Morii</i>	

Hash Functions

Time-Memory Trade-Offs for Near-Collisions 205
Gaëtan Leurent

Collision Attacks on Up to 5 Rounds of SHA-3 Using Generalized
 Internal Differentials 219
Itai Dinur, Orr Dunkelman, and Adi Shamir

Rotational Cryptanalysis of Round-Reduced KECCAK 241
Paweł Morawiecki, Josef Pieprzyk, and Marian Srebrny

Partial-Collision Attack on the Round-Reduced Compression Function
 of Skein-256 263
Hongbo Yu, Jiazhe Chen, and Xiaoyun Wang

Message Authentication Codes

On Weak Keys and Forgery Attacks Against Polynomial-Based
 MAC Schemes 287
Gordon Procter and Carlos Cid

Secure Message Authentication Against Related-Key Attack 305
Rishiraj Bhattacharyya and Arnab Roy

Provable Security

Attacks and Security Proofs of EAX-Prime 327
Kazuhiko Minematsu, Stefan Lucks, Hiraku Morita, and Tetsu Iwata

Towards Understanding the Known-Key Security of Block Ciphers 348
Elena Andreeva, Andrey Bogdanov, and Bart Mennink

On Symmetric Encryption with Distinguishable Decryption Failures 367
*Alexandra Boldyreva, Jean Paul Degabriele, Kenneth G. Paterson,
 and Martijn Stam*

Implementation Aspects

Minimalism of Software Implementation 393
Mitsuru Matsui and Yumiko Murakami

Higher-Order Side Channel Security and Mask Refreshing 410
*Jean-Sébastien Coron, Emmanuel Prouff, Matthieu Rivain,
 and Thomas Roche*

Masking Tables—An Underestimated Security Risk 425
Michael Tunstall, Carolyn Whitnall, and Elisabeth Oswald

Lightweight Authenticated Encryption

ALE: AES-Based Lightweight Authenticated Encryption. 447
Andrey Bogdanov, Florian Mendel, Francesco Regazzoni, Vincent Rijmen, and Elmar Tischhauser

Related-Key Attacks Against Full Hummingbird-2 467
Markku-Juhani O. Saarinen

Stream Ciphers II

A Low Data Complexity Attack on the GMR-2 Cipher Used
in the Satellite Phones. 485
Ruilin Li, Heng Li, Chao Li, and Bing Sun

Improving Key Recovery to 784 and 799 Rounds of Trivium
Using Optimized Cube Attacks. 502
Pierre-Alain Fouque and Thomas Vannet

Near Collision Attack on the Grain v1 Stream Cipher. 518
Bin Zhang, Zhenqi Li, Dengguo Feng, and Dongdai Lin

Automated Cryptanalysis

Exhausting Demirci-Seuk Meet-in-the-Middle Attacks Against
Reduced-Round AES. 541
Patrick Derbez and Pierre-Alain Fouque

A Framework for Automated Independent-Biclique Cryptanalysis 561
Farzaneh Abed, Christian Forler, Eik List, Stefan Lucks, and Jakob Wenzel

Boolean Functions

A New Criterion for Avoiding the Propagation of Linear Relations
Through an Sbox 585
Christina Boura and Anne Canteaut

Author Index 605



<http://www.springer.com/978-3-662-43932-6>

Fast Software Encryption

20th International Workshop, FSE 2013, Singapore,

March 11-13, 2013. Revised Selected Papers

Moriai, S. (Ed.)

2014, XIII, 605 p. 135 illus., Softcover

ISBN: 978-3-662-43932-6