

Table of Contents

Hash Functions I

Zero-Sum Distinguishers for Iterated Permutations and Application to KECCAK- f and Hamsi-256	1
<i>Christina Boura and Anne Canteaut</i>	
Attacks on Hash Functions Based on Generalized Feistel: Application to Reduced-Round <i>Lesamnta</i> and <i>SHAvite-3</i> ₅₁₂	18
<i>Charles Bouillaguet, Orr Dunkelman, Gaëtan Leurent, and Pierre-Alain Fouque</i>	
The Differential Analysis of S-Functions	36
<i>Nicky Mouha, Vesselin Velichkov, Christophe De Cannière, and Bart Preneel</i>	

Stream Ciphers

Hill Climbing Algorithms and Trivium	57
<i>Julia Borghoff, Lars R. Knudsen, and Krystian Matusiewicz</i>	
Discovery and Exploitation of New Biases in RC4	74
<i>Pouyan Sepehrdad, Serge Vaudenay, and Martin Vuagnoux</i>	

The Stafford Tavares Lecture

The Rise and Fall and Rise of Combinatorial Key Predistribution	92
<i>Keith M. Martin</i>	

Efficient Implementations

A Low-Area Yet Performant FPGA Implementation of Shabal	99
<i>Jérémy Detrey, Pierrick Gaudry, and Karim Khalfallah</i>	
Implementation of Symmetric Algorithms on a Synthesizable 8-Bit Microcontroller Targeting Passive RFID Tags	114
<i>Thomas Plos, Hannes Groß, and Martin Feldhofer</i>	
Batch Computations Revisited: Combining Key Computations and Batch Verifications	130
<i>René Struik</i>	

Coding and Combinatorics

Wild McEliece	143
<i>Daniel J. Bernstein, Tanja Lange, and Christiane Peters</i>	
Parallel-CFS: Strengthening the CFS McEliece-Based Signature Scheme	159
<i>Matthieu Finiasz</i>	
A Zero-Knowledge Identification Scheme Based on the q-ary Syndrome Decoding Problem	171
<i>Pierre-Louis Cayrel, Pascal Véron, and Sidi Mohamed El Yousfi Alaoui</i>	
Optimal Covering Codes for Finding Near-Collisions	187
<i>Mario Lamberger and Vincent Rijmen</i>	

Block Ciphers

Tweaking AES	198
<i>Ivica Nikolić</i>	
On the Diffusion of Generalized Feistel Structures Regarding Differential and Linear Cryptanalysis	211
<i>Kyoji Shibutani</i>	
A 3-Subset Meet-in-the-Middle Attack: Cryptanalysis of the Lightweight Block Cipher KTANTAN	229
<i>Andrey Bogdanov and Christian Rechberger</i>	

Side Channel Attacks

Improving DPA by Peak Distribution Analysis	241
<i>Jing Pan, Jasper G.J. van Woudenberg, Jerry I. den Hartog, and Marc F. Witteman</i>	
Affine Masking against Higher-Order Side Channel Analysis	262
<i>Guillaume Fumarolet, Ange Martinelli, Emmanuel Prouff, and Matthieu Rivain</i>	

Invited Talk

Search on Encrypted Data in the Symmetric-Key Setting	281
<i>Alexandra Boldyreva</i>	

Mathematical Aspects

Preimages for the Tillich-Zémor Hash Function	282
<i>Christophe Petit and Jean-Jacques Quisquater</i>	
One-Time Signatures and Chameleon Hash Functions.....	302
<i>Payman Mohassel</i>	
On the Minimum Communication Effort for Secure Group Key Exchange	320
<i>Frederik Armknecht and Jun Furukawa</i>	

Hash Functions II

Deterministic Differential Properties of the Compression Function of BMW	338
<i>Jian Guo and Søren S. Thomsen</i>	
Security Analysis of SIMD.....	351
<i>Charles Bouillaguet, Pierre-Alain Fouque, and Gaëtan Leurent</i>	
Subspace Distinguisher for 5/8 Rounds of the ECHO-256 Hash Function	369
<i>Martin Schläffer</i>	
Cryptanalysis of <i>Luffa</i> v2 Components.....	388
<i>Dmitry Khovratovich, María Naya-Plasencia, Andrea Röck, and Martin Schläffer</i>	
Author Index	411