

Table of Contents

Invited Talk

- Getting a Few Things Right and Many Things Wrong 1
Neal Koblitz

Security of RSA and Multivariate Schemes

- Partial Key Exposure Attack on RSA – Improvements for Limited
Lattice Dimensions 2
Santanu Sarkar, Sourav Sen Gupta, and Subhamoy Maitra
- Towards Provable Security of the Unbalanced Oil and Vinegar
Signature Scheme under Direct Attacks 17
Stanislav Bulygin, Albrecht Petzoldt, and Johannes Buchmann
- CyclicRainbow – A Multivariate Signature Scheme with a Partially
Cyclic Public Key 33
Albrecht Petzoldt, Stanislav Bulygin, and Johannes Buchmann

Security Analysis, Pseudorandom Permutations and Applications

- Combined Security Analysis of the One- and Three-Pass Unified Model
Key Agreement Protocols 49
Sanjit Chatterjee, Alfred Menezes, and Berkant Ustaoglu
- Indifferentiability beyond the Birthday Bound for the Xor of Two
Public Random Permutations 69
Avradip Mandal, Jacques Patarin, and Valerie Nachev
- The Characterization of Luby-Rackoff and Its Optimum Single-Key
Variants 82
Mridul Nandi
- Versatile Prêt à Voter: Handling Multiple Election Methods with a
Unified Interface 98
*Zhe Xia, Chris Culnane, James Heather, Hugo Jonker,
Peter Y.A. Ryan, Steve Schneider, and Sriramkrishnan Srinivasan*

Invited Talk

- Cryptographic Hash Functions: Theory and Practice 115
Bart Preneel

Hash Functions

Cryptanalysis of Tav-128 Hash Function	118
<i>Ashish Kumar, Somitra Kumar Sanadhy, Praveen Gauravaram, Masoumeh Safkhani, and Majid Naderi</i>	
Near-Collisions for the Reduced Round Versions of Some Second Round SHA-3 Compression Functions Using Hill Climbing	131
<i>Meltem Sönmez Turan and Erdener Uyan</i>	
Speeding Up the Wide-Pipe: Secure and Fast Hashing	144
<i>Mridul Nandi and Souradyuti Paul</i>	

Attacks on Block Ciphers and Stream Ciphers

New Boomerang Attacks on ARIA	163
<i>Ewan Fleischmann, Christian Forler, Michael Gorski, and Stefan Lucks</i>	
Algebraic, AIDA/Cube and Side Channel Analysis of KATAN Family of Block Ciphers	176
<i>Gregory V. Bard, Nicolas T. Courtois, Jorge Nakahara Jr., Pouyan Sepehrdad, and Bingsheng Zhang</i>	
The Improbable Differential Attack: Cryptanalysis of Reduced Round CLEFIA	197
<i>Cihangir Tezcan</i>	
Greedy Distinguishers and Nonrandomness Detectors	210
<i>Paul Stankovski</i>	

Fast Cryptographic Computation

Polynomial Multiplication over Binary Fields Using Charlier Polynomial Representation with Low Space Complexity	227
<i>Sedat Akleylek, Murat Cenk, and Ferruh Özbudak</i>	
Random Euclidean Addition Chain Generation and Its Application to Point Multiplication	238
<i>Fabien Herbaut, Pierre-Yvan Liardet, Nicolas Méloni, Yannick Téglia, and Pascal Véron</i>	

Cryptanalysis of AES

Attack on a Higher-Order Masking of the AES Based on Homographic Functions	262
<i>Emmanuel Prouff and Thomas Roche</i>	

Improved Impossible Differential Cryptanalysis of 7-Round AES-128	282
<i>Hamid Mala, Mohammad Dakhilalian, Vincent Rijmen, and Mahmoud Modarres-Hashemi</i>	

Cryptanalysis of a Perturbated White-Box AES Implementation	292
<i>Yoni De Mulder, Brecht Wyseur, and Bart Preneel</i>	

Efficient Implementation

A Program Generator for Intel AES-NI Instructions	311
<i>Raymond Manley and David Gregg</i>	

ECC2K-130 on NVIDIA GPUs	328
<i>Daniel J. Bernstein, Hsieh-Chung Chen, Chen-Mou Cheng, Tanja Lange, Ruben Niederhagen, Peter Schwabe, and Bo-Yin Yang</i>	

One Byte per Clock: A Novel RC4 Hardware	347
<i>Sourav Sen Gupta, Koushik Sinha, Subhamoy Maitra, and Bhabani P. Sinha</i>	

Author Index	365
------------------------	-----