

Table of Contents – Part I

Cryptology and Coding Theory

Solving LPN Using Covering Codes	1
<i>Qian Guo, Thomas Johansson, and Carl Löndahl</i>	
Algebraic Attack against Variants of McEliece with Goppa Polynomial of a Special Form	21
<i>Jean-Charles Faugère, Ludovic Perret, and Frédéric de Portzamparc</i>	

New Proposals

Bivariate Polynomials Modulo Composites and Their Applications	42
<i>Dan Boneh and Henry Corrigan-Gibbs</i>	
Cryptographic Schemes Based on the ASASA Structure: Black-box, White-box, and Public-key (Extended Abstract)	63
<i>Alex Biryukov, Charles Bouillaguet, and Dmitry Khovratovich</i>	

Authenticated Encryption

Beyond $2^{c/2}$ Security in Sponge-Based Authenticated Encryption Modes	85
<i>Philipp Jovanovic, Atul Luykx, and Bart Mennink</i>	
How to Securely Release Unverified Plaintext in Authenticated Encryption	105
<i>Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink, Nicky Mouha, and Kan Yasuda</i>	

Forging Attacks on Two Authenticated Encryption Schemes COBRA and POET	126
<i>Mridul Nandi</i>	

Symmetric Key Cryptanalysis

Low Probability Differentials and the Cryptanalysis of Full-Round CLEFIA-128	141
<i>Sareh Emami, San Ling, Ivica Nikolić, Josef Pieprzyk, and Huaxiong Wang</i>	

Automatic Security Evaluation and (Related-key) Differential Characteristic Search: Application to SIMON, PRESENT, LBlock, DES(L) and Other Bit-Oriented Block Ciphers	158
<i>Siwei Sun, Lei Hu, Peng Wang, Kexin Qiao, Xiaoshuang Ma, and Ling Song</i>	
Scrutinizing and Improving Impossible Differential Attacks: Applications to CLEFIA, Camellia, LBlock and SIMON	179
<i>Christina Boura, María Naya-Plasencia, and Valentin Suder</i>	
A Simplified Representation of AES	200
<i>Henri Gilbert</i>	
Side Channel Analysis I	
Simulatable Leakage: Analysis, Pitfalls, and New Constructions	223
<i>Jake Longo, Daniel P. Martin, Elisabeth Oswald, Daniel Page, Martijin Stam, and Michael J. Tunstall</i>	
Multi-target DPA Attacks: Pushing DPA Beyond the Limits of a Desktop Computer	243
<i>Luke Mather, Elisabeth Oswald, and Carolyn Whitnall</i>	
GLV/GLS Decomposition, Power Analysis, and Attacks on ECDSA Signatures with Single-Bit Nonce Bias	262
<i>Diego F. Aranha, Pierre-Alain Fouque, Benoît Gérard, Jean-Gabriel Kammerer, Mehdi Tibouchi, and Jean-Christophe Zapalowicz</i>	
Soft Analytical Side-Channel Attacks	282
<i>Nicolas Veyrat-Charvillon, Benoît Gérard, and François-Xavier Standaert</i>	
Hyperelliptic Curve Cryptography	
On the Enumeration of Double-Base Chains with Applications to Elliptic Curve Cryptography	297
<i>Christophe Doche</i>	
Kummer Strikes Back: New DH Speed Records	317
<i>Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Peter Schwabe</i>	
Jacobian Coordinates on Genus 2 Curves	338
<i>Huseyin Hisil and Craig Costello</i>	

Factoring and Discrete Log

Mersenne Factorization Factory	358
<i>Thorsten Kleinjung, Joppe W. Bos, and Arjen K. Lenstra</i>	

Improving the Polynomial time Precomputation of Frobenius Representation Discrete Logarithm Algorithms: Simplified Setting for Small Characteristic Finite Fields	378
<i>Antoine Joux and Cécile Pierrot</i>	

Invited Talk I

Big Bias Hunting in Amazonia: Large-Scale Computation and Exploitation of RC4 Biases (Invited Paper)	398
<i>Kenneth G. Paterson, Bertram Poettering, and Jacob C.N. Schuldt</i>	

Cryptanalysis

Multi-user Collisions: Applications to Discrete Logarithm, Even-Mansour and PRINCE	420
<i>Pierre-Alain Fouque, Antoine Joux, and Chrysanthi Mavromati</i>	

Cryptanalysis of Iterated Even-Mansour Schemes with Two Keys	439
<i>Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir</i>	

Meet-in-the-Middle Attacks on Generic Feistel Constructions	458
<i>Jian Guo, Jérémie Jean, Ivica Nikolić, and Yu Sasaki</i>	

XLS is Not a Strong Pseudorandom Permutation	478
<i>Mridul Nandi</i>	

Signatures

Structure-Preserving Signatures on Equivalence Classes and Their Application to Anonymous Credentials	491
<i>Christian Hanser and Daniel Slamanig</i>	

On Tight Security Proofs for Schnorr Signatures	512
<i>Nils Fleischhacker, Tibor Jager, and Dominique Schröder</i>	

Zero-Knowledge

Square Span Programs with Applications to Succinct NIZK Arguments	532
<i>George Danezis, Cédric Fournet, Jens Groth, and Markulf Kohlweiss</i>	

Better Zero-Knowledge Proofs for Lattice Encryption and Their Application to Group Signatures	551
<i>Fabrice Benhamouda, Jan Camenisch, Stephan Krenn, Vadim Lyubashevsky, and Gregory Neven</i>	
Author Index	573