

Table of Contents

Cryptanalysis

A New Related Message Attack on RSA	1
<i>Oded Yacobi and Yacov Yacobi</i>	
Breaking a Cryptographic Protocol with Pseudoprimes	9
<i>Daniel Bleichenbacher</i>	
Experimenting with Faults, Lattices and the DSA	16
<i>David Naccache, Phong Q. Nguyễn, Michael Tunstall, and Claire Whelan</i>	

Key Establishment

Securing RSA-KEM via the AES	29
<i>Jakob Jonsson and Matthew J.B. Robshaw</i>	
One-Time Verifier-Based Encrypted Key Exchange	47
<i>Michel Abdalla, Olivier Chevassut, and David Pointcheval</i>	
Password-Based Authenticated Key Exchange in the Three-Party Setting	65
<i>Michel Abdalla, Pierre-Alain Fouque, and David Pointcheval</i>	

Optimization

On the Optimization of Side-Channel Attacks by Advanced Stochastic Methods	85
<i>Werner Schindler</i>	
Symmetric Subgroup Membership Problems	104
<i>Kristian Gjøsteen</i>	

Building Blocks

Optimizing Robustness While Generating Shared Secret Safe Primes	120
<i>Emil Ong and John Kubiawicz</i>	
Fast Multi-computations with Integer Similarity Strategy	138
<i>Wu-Chuan Yang, Dah-Jyh Guan, and Chi-Sung Laih</i>	

Efficient Proofs of Knowledge of Discrete Logarithms and Representations
in Groups with Hidden Order 154
Endre Bangerter, Jan Camenisch, and Ueli Maurer

Efficient k -Out-of- n Oblivious Transfer Schemes
with Adaptive and Non-adaptive Queries 172
Cheng-Kang Chu and Wen-Guey Tzeng

RSA Cryptography

Converse Results to the Wiener Attack on RSA 184
Ron Steinfeld, Scott Contini, Huaxiong Wang, and Josef Pieprzyk

RSA with Balanced Short Exponents and Its Application
to Entity Authentication 199
Hung-Min Sun and Cheng-Ta Yang

The Sampling Twice Technique for the RSA-Based Cryptosystems
with Anonymity 216
Ryotaro Hayashi and Keisuke Tanaka

From Fixed-Length to Arbitrary-Length
RSA Encoding Schemes Revisited 234
Julien Cathalo, Jean-Sébastien Coron, and David Naccache

Multivariate Asymmetric Cryptography

Tractable Rational Map Signature 244
*Lih-Chung Wang, Yuh-Hua Hu, Feipei Lai, Chun-Yen Chou,
and Bo-Yin Yang*

Cryptanalysis of the Tractable Rational Map Cryptosystem 258
*Antoine Joux, Sébastien Kunz-Jacques, Frédéric Muller,
and Pierre-Michel Ricordel*

Large Superfluous Keys in Multivariate Quadratic Asymmetric Systems . . 275
Christopher Wolf and Bart Preneel

Cryptanalysis of HFEv and Internal Perturbation of HFE 288
Jintai Ding and Dieter Schmidt

Signature Schemes

A Generic Scheme Based on Trapdoor One-Way Permutations
with Signatures as Short as Possible 302
Louis Granboulan

Cramer-Damgård Signatures Revisited: Efficient Flat-Tree Signatures Based on Factoring	313
<i>Dario Catalano and Rosario Gennaro</i>	

The Security of the FDH Variant of Chaum's Undeniable Signature Scheme	328
<i>Wakaha Ogata, Kaoru Kurosawa, and Swee-Huay Heng</i>	

Efficient Threshold RSA Signatures with General Moduli and No Extra Assumptions	346
<i>Ivan Damgård and Kasper Dupont</i>	

Identity-Based Cryptography

Improved Identity-Based Signcryption	362
<i>Liqun Chen and John Malone-Lee</i>	

Efficient Multi-receiver Identity-Based Encryption and Its Application to Broadcast Encryption	380
<i>Joonsang Baek, Reihaneh Safavi-Naini, and Willy Susilo</i>	

CBE from CL-PKE: A Generic Construction and Efficient Schemes	398
<i>Sattam S. Al-Riyami and Kenneth G. Paterson</i>	

Best Paper Award

A Verifiable Random Function with Short Proofs and Keys	416
<i>Yevgeniy Dodis and Aleksandr Yampolskiy</i>	

Author Index	433
---------------------------	-----