

# 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 Lai</i>	

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

Efficient $k$ -Out-of- $n$ Oblivious Transfer Schemes with Adaptive and Non-adaptive Queries . . . . .	172
<i>Cheng-Kang Chu and Wen-Guey Tzeng</i>	

## RSA Cryptography

Converse Results to the Wiener Attack on RSA . . . . .	184
<i>Ron Steinfeld, Scott Contini, Huaxiong Wang, and Josef Pieprzyk</i>	

RSA with Balanced Short Exponents and Its Application to Entity Authentication . . . . .	199
<i>Hung-Min Sun and Cheng-Ta Yang</i>	

The Sampling Twice Technique for the RSA-Based Cryptosystems with Anonymity . . . . .	216
<i>Ryotaro Hayashi and Keisuke Tanaka</i>	

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

## Multivariate Asymmetric Cryptography

Tractable Rational Map Signature . . . . .	244
<i>Lih-Chung Wang, Yuh-Hua Hu, Feipei Lai, Chun-Yen Chou, and Bo-Yin Yang</i>	

Cryptanalysis of the Tractable Rational Map Cryptosystem . . . . .	258
<i>Antoine Joux, Sébastien Kunz-Jacques, Frédéric Muller, and Pierre-Michel Ricordel</i>	

Large Superfluous Keys in Multivariate Quadratic Asymmetric Systems . .	275
<i>Christopher Wolf and Bart Preneel</i>	

Cryptanalysis of HFEv and Internal Perturbation of HFE . . . . .	288
<i>Jintai Ding and Dieter Schmidt</i>	

## Signature Schemes

A Generic Scheme Based on Trapdoor One-Way Permutations with Signatures as Short as Possible . . . . .	302
<i>Louis Granboulan</i>	

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>	
<b>Author Index</b> .....	433

Public Key Cryptography - PKC 2005

8th International Workshop on Theory and Practice in

Public Key Cryptography

Vaudenay, S. (Ed.)

2005, XIV, 436 p., Softcover

ISBN: 978-3-540-24454-7