Public Key Cryptography – PKC 2007

10th International Conference on Practice and Theory in Public-Key Cryptography
Beijing, China, April 16-20, 2007
Proceedings
Table of Contents

Signatures I

Full-Domain Subgroup Hiding and Constant-Size Group Signatures ..... 1
Xavier Boyen and Brent Waters

A Direct Anonymous Attestation Scheme for Embedded Devices ..... 16
He Ge and Stephen R. Tate

Anonymous Signatures Made Easy .................................................. 31
Marc Fischlin

On the Generic and Efficient Constructions of Secure Designated
Confirmers Signatures ................................................................. 43
Guilin Wang, Joonsang Baek, Duncan S. Wong, and Feng Bao

Invited Talk I

Cryptanalysis of Group-Based Key Agreement Protocols Using
Subgroup Distance Functions .......................................................... 61
Dima Ruinskiy, Adi Shamir, and Boaz Tsaban

Cryptanalysis

Length Based Attack and Braid Groups: Cryptanalysis of
Anshel-Anshel-Goldfeld Key Exchange Protocol ............................... 76
Alex D. Myasnikov and Alexander Ushakov

New Chosen-Ciphertext Attacks on NTRU ................................. 89
Nicolas Gama and Phong Q. Nguyen

Cryptanalysis of the Paeng-Jung-Ha Cryptosystem from PKC 2003 ..... 107
Daewan Han, Myung-Hwan Kim, and Yongjin Yeom

Protocols I

Optimistic Fair Exchange in a Multi-user Setting ...................... 118
Yevgeniy Dodis, Pil Joong Lee, and Dae Hyun Yum

Multi-party Stand-Alone and Setup-Free Verifiably Committed
Signatures .................................................................................. 134
Huafei Zhu, Willy Susilo, and Yi Mu

Knowledge-Binding Commitments with Applications in
Time-Stamping ........................................................................ 150
Ahto Buldas and Sven Laur
# Signatures II

Efficient Ring Signatures Without Random Oracles .................................. 166  
*Hovav Shacham and Brent Waters*

Traceable Ring Signature .......................................................... 181  
*Eiichiro Fujisaki and Koutarou Suzuki*

Two-Tier Signatures, Strongly Unforgeable Signatures, and Fiat-Shamir Without Random Oracles ................................. 201  
*Mihir Bellare and Sarah Shoup*

Improved On-Line/Off-Line Threshold Signatures .................................. 217  
*Emmanuel Bresson, Dario Catalano, and Rosario Gennaro*

# Multivariate Cryptosystems

High Order Linearization Equation (HOLE) Attack on Multivariate Public Key Cryptosystems ........................................... 233  
*Jintai Ding, Lei Hu, Xuyun Nie, Jianyu Li, and John Wagner*

Cryptanalysis of HFE with Internal Perturbation ................................ 249  
*Vivien Dubois, Louis Granboulan, and Jacques Stern*

$\ell$-Invertible Cycles for Multivariate Quadratic ($\mathcal{MQ}$) Public Key Cryptography ......................................................... 266  
*Jintai Ding, Christopher Wolf, and Bo-Yin Yang*

# Encryption

Chosen-Ciphertext Secure Key-Encapsulation Based on Gap Hashed Diffie-Hellman ....................................................... 282  
*Eike Kiltz*

Parallel Key-Insulated Public Key Encryption Without Random Oracles ................................................................. 298  
*Benoît Libert, Jean-Jacques Quisquater, and Moti Yung*

Multi-bit Cryptosystems Based on Lattice Problems ................................... 315  
*Akinori Kawachi, Keisuke Tanaka, and Keita Xagawa*

# Protocols II

Practical and Secure Solutions for Integer Comparison ......................... 330  
*Juan Garay, Berry Schoenmakers, and José Villegas*

Multiparty Computation for Interval, Equality, and Comparison Without Bit-Decomposition Protocol .............................. 343  
*Takashi Nishide and Kazuo Ohta*
Identity-Based Traitor Tracing ........................................... 361
  Michel Abdalla, Alexander W. Dent, John Malone-Lee,  
  Gregory Neven, Duong Hieu Phan, and Nigel P. Smart

Verifiable Shuffle of Large Size Ciphertexts ......................... 377
  Jens Groth and Steve Lu

Invited Talk II

A Survey of Single-Database Private Information Retrieval: Techniques  
and Applications .......................................................... 393
  Rafail Ostrovsky and William E. Skeith III

Number Theoretic Techniques

Deterministic Polynomial Time Equivalence Between Factoring and  
Key-Recovery Attack on Takagi's RSA .................................. 412
  Noboru Kunihiro and Kaoru Kurosawa

Efficient Pseudorandom Generators Based on the DDH Assumption ... 426
  Reza Rezaeian Farashahi, Berry Schoenmakers, and  
  Andrey Sidorenko

Fast Batch Verification of Multiple Signatures ....................... 442
  Jung Hee Cheon and Jeong Hyun Yi

Public-Key Infrastructure

A Closer Look at PKI: Security and Efficiency .......................... 458
  Alexandra Boldyreva, Marc Fischlin, Adriana Palacio, and  
  Bogdan Warinschi

Self-Generated-Certificate Public Key Encryption Without Pairing ... 476
  Junzuo Lai and Weidong Kou

Author Index ................................................................. 491