

Table of Contents

Diffie-Hellman Based Schemes

Efficient Construction of (Distributed) Verifiable Random Functions	1
<i>Yevgeniy Dodis</i>	
An Identity-Based Signature from Gap Diffie-Hellman Groups	18
<i>Jae Choon Cha and Jung Hee Cheon</i>	

Threshold Cryptography

Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme	31
<i>Alexandra Boldyreva</i>	
An Efficient Two-Party Public Key Cryptosystem Secure against Adaptive Chosen Ciphertext Attack	47
<i>Philip MacKenzie</i>	

Reduction Proofs

On the Bit Security of NTRUEncrypt	62
<i>Mats Näslund, Igor E. Shparlinski, and William Whyte</i>	
Equivalence between Semantic Security and Indistinguishability against Chosen Ciphertext Attacks	71
<i>Yodai Watanabe, Junji Shikata, and Hideki Imai</i>	

Broadcast and Tracing

Randomness Re-use in Multi-recipient Encryption Schemes	85
<i>Mihir Bellare, Alexandra Boldyreva, and Jessica Staddon</i>	
Public Key Trace and Revoke Scheme Secure against Adaptive Chosen Ciphertext Attack	100
<i>Yevgeniy Dodis and Nelly Fazio</i>	

Digital Signatures

The Cramer-Shoup Strong-RSA Signature Scheme Revisited	116
<i>Marc Fischlin</i>	
Strong Key-Insulated Signature Schemes	130
<i>Yevgeniy Dodis, Jonathan Katz, Shouhuai Xu, and Moti Yung</i>	

Specialized Multiparty Cryptography

A Verifiable Secret Shuffle of Homomorphic Encryptions	145
<i>Jens Groth</i>	
Round-Optimal Contributory Conference Key Agreement	161
<i>Colin Boyd and Juan Manuel González Nieto</i>	

Cryptanalysis I

Security Analysis of the MOR Cryptosystem	175
<i>Christian Tobias</i>	
A Practical Attack on Some Braid Group Based Cryptographic Primitives	187
<i>Dennis Hofheinz and Rainer Steinwandt</i>	

Elliptic Curves: Implementation Attacks

A Refined Power-Analysis Attack on Elliptic Curve Cryptosystems	199
<i>Louis Goubin</i>	
Validation of Elliptic Curve Public Keys	211
<i>Adrian Antipa, Daniel Brown, Alfred Menezes, René Struik, and Scott Vanstone</i>	
Exceptional Procedure Attack on Elliptic Curve Cryptosystems	224
<i>Tetsuya Izu and Tsuyoshi Takagi</i>	

Implementation and Hardware Issues

On Montgomery-Like Representations for Elliptic Curves over $GF(2^k)$	240
<i>Martijn Stam</i>	
A Dedicated Sieving Hardware	254
<i>Willi Geiselmann and Rainer Steinwandt</i>	
A Fast and Secure Implementation of Sflash	267
<i>Mehdi-Laurent Akkar, Nicolas T. Courtois, Romain Duteuil, and Louis Goubin</i>	

New Public Key Schemes

A Practical Public Key Cryptosystem from Paillier and Rabin Schemes ...	279
<i>David Galindo, Sebastià Martín, Paz Morillo, and Jorge L. Villar</i>	
A Lattice Based Public Key Cryptosystem Using Polynomial Representations	292
<i>Seong-Hun Paeng, Bae Eun Jung, and Kil-Chan Ha</i>	

Elliptic Curves: General Issues

The Security of DSA and ECDSA (Bypassing the Standard Elliptic Curve Certification Scheme)	309
<i>Serge Vaudenay</i>	

Cryptanalysis II

Side-Channel Attacks on Textbook RSA and ElGamal Encryption	324
<i>Ulrich Kühn</i>	
On the Security of HFE, HFEv- and Quartz	337
<i>Nicolas T. Courtois, Magnus Daum, and Patrick Felke</i>	
Generic Attacks and the Security of Quartz	351
<i>Nicolas T. Courtois</i>	
Author Index	365

Public Key Cryptography - PKC 2003

6th International Workshop on Theory and Practice in

Public Key Cryptography, Miami, FL, USA, January 6-8,

2003, Proceedings

Desmedt, Y. (Ed.)

2002, XII, 376 p., Softcover

ISBN: 978-3-540-00324-3