

Table of Contents

Diffie-Hellman Based Schemes

- Efficient Construction of (Distributed) Verifiable Random Functions1
Yevgeniy Dodis
- An Identity-Based Signature from Gap Diffie-Hellman Groups18
Jae Choon Cha and Jung Hee Cheon

Threshold Cryptography

- Threshold Signatures, Multisignatures and Blind Signatures Based
on the Gap-Diffie-Hellman-Group Signature Scheme31
Alexandra Boldyreva
- An Efficient Two-Party Public Key Cryptosystem Secure
against Adaptive Chosen Ciphertext Attack47
Philip MacKenzie

Reduction Proofs

- On the Bit Security of NTRUEncrypt62
Mats Näslund, Igor E. Shparlinski, and William Whyte
- Equivalence between Semantic Security and Indistinguishability
against Chosen Ciphertext Attacks71
Yodai Watanabe, Junji Shikata, and Hideki Imai

Broadcast and Tracing

- Randomness Re-use in Multi-recipient Encryption Schemes 85
Mihir Bellare, Alexandra Boldyreva, and Jessica Staddon
- Public Key Trace and Revoke Scheme Secure
against Adaptive Chosen Ciphertext Attack100
Yevgeniy Dodis and Nelly Fazio

Digital Signatures

- The Cramer-Shoup Strong-RSA Signature Scheme Revisited 116
Marc Fischlin
- Strong Key-Insulated Signature Schemes130
Yevgeniy Dodis, Jonathan Katz, Shouhuai Xu, and Moti Yung

Specialized Multiparty Cryptography

A Verifiable Secret Shuffle of Homomorphic Encryptions 145
Jens Groth

Round-Optimal Contributory Conference Key Agreement 161
Colin Boyd and Juan Manuel González Nieto

Cryptanalysis I

Security Analysis of the MOR Cryptosystem 175
Christian Tobias

A Practical Attack on Some Braid Group
Based Cryptographic Primitives 187
Dennis Hofheinz and Rainer Steinwandt

Elliptic Curves: Implementation Attacks

A Refined Power-Analysis Attack on Elliptic Curve Cryptosystems 199
Louis Goubin

Validation of Elliptic Curve Public Keys 211
*Adrian Antipa, Daniel Brown, Alfred Menezes, René Struik,
and Scott Vanstone*

Exceptional Procedure Attack on Elliptic Curve Cryptosystems 224
Tetsuya Izu and Tsuyoshi Takagi

Implementation and Hardware Issues

On Montgomery-Like Representations for Elliptic Curves over $GF(2^k)$ 240
Martijn Stam

A Dedicated Sieving Hardware 254
Willi Geiselmann and Rainer Steinwandt

A Fast and Secure Implementation of Sflash 267
*Mehdi-Laurent Akkar, Nicolas T. Courtois, Romain Duteuil,
and Louis Goubin*

New Public Key Schemes

A Practical Public Key Cryptosystem from Paillier and Rabin Schemes ... 279
David Galindo, Sebastià Martín, Paz Morillo, and Jorge L. Villar

A Lattice Based Public Key Cryptosystem
Using Polynomial Representations 292
Seong-Hun Paeng, Bae Eun Jung, and Kil-Chan Ha

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