

# Table of Contents

A Generalized Wiener Attack on RSA .....	1
<i>Johannes Blömer and Alexander May</i>	
Cryptanalysis of a Public-Key Encryption Scheme Based on the Polynomial Reconstruction Problem .....	14
<i>Jean-Sébastien Coron</i>	
Faster Scalar Multiplication on Koblitz Curves Combining Point Halving with the Frobenius Endomorphism .....	28
<i>Roberto Maria Avanzi, Mathieu Ciet, and Francesco Sica</i>	
Application of Montgomery's Trick to Scalar Multiplication for Elliptic and Hyperelliptic Curves Using a Fixed Base Point .....	41
<i>Pradeep Kumar Mishra and Palash Sarkar</i>	
Fast Arithmetic on Jacobians of Picard Curves .....	55
<i>Stéphane Flon and Roger Oyono</i>	
Undeniable Signatures Based on Characters: How to Sign with One Bit ..	69
<i>Jean Monnerat and Serge Vaudenay</i>	
Efficient Extension of Standard Schnorr/RSA Signatures into Universal Designated-Verifier Signatures .....	86
<i>Ron Steinfeld, Huaxiong Wang, and Josef Pieprzyk</i>	
Constructing Committed Signatures from Strong-RSA Assumption in the Standard Complexity Model .....	101
<i>Huafei Zhu</i>	
Constant Round Authenticated Group Key Agreement via Distributed Computation .....	115
<i>Emmanuel Bresson and Dario Catalano</i>	
Efficient ID-based Group Key Agreement with Bilinear Maps .....	130
<i>Kyu Young Choi, Jung Yeon Hwang, and Dong Hoon Lee</i>	
New Security Results on Encrypted Key Exchange .....	145
<i>Emmanuel Bresson, Olivier Chevassut, and David Pointcheval</i>	
New Results on the Hardness of Diffie-Hellman Bits .....	159
<i>María Isabel González Vasco, Mats Näslund, and Igor E. Shparlinski</i>	
Short Exponent Diffie-Hellman Problems .....	173
<i>Takeshi Koshihara and Kaoru Kurosawa</i>	

Efficient Signcryption with Key Privacy from Gap Diffie-Hellman Groups . . . . .	187
<i>Benoît Libert and Jean-Jacques Quisquater</i>	
Algebraic Attacks over $GF(2^k)$ , Application to HFE Challenge 2 and Sflash-v2 . . . . .	201
<i>Nicolas T. Courtois</i>	
Secret Exponent Attacks on RSA-type Schemes with Moduli $N = p^r q$ . . .	218
<i>Alexander May</i>	
General Group Authentication Codes and Their Relation to “Unconditionally-Secure Signatures” . . . . .	231
<i>Reihaneh Safavi-Naini, Luke McAven, and Moti Yung</i>	
From Digital Signature to ID-based Identification/Signature . . . . .	248
<i>Kaoru Kurosawa and Swee-Huay Heng</i>	
Identity-Based Threshold Decryption . . . . .	262
<i>Joonsang Baek and Yuliang Zheng</i>	
An Efficient Signature Scheme from Bilinear Pairings and Its Applications . . . . .	277
<i>Fanguo Zhang, Reihaneh Safavi-Naini, and Willy Susilo</i>	
An RSA Family of Trap-Door Permutations with a Common Domain and Its Applications . . . . .	291
<i>Ryotaro Hayashi, Tatsuaki Okamoto, and Keisuke Tanaka</i>	
A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation . . . . .	305
<i>Jintai Ding</i>	
Efficient, Verifiable Shuffle Decryption and Its Requirement of Unlinkability . . . . .	319
<i>Jun Furukawa</i>	
A Point Compression Method for Elliptic Curves Defined over $GF(2^n)$ . . .	333
<i>Brian King</i>	
On the Optimal Parameter Choice for Elliptic Curve Cryptosystems Using Isogeny . . . . .	346
<i>Toru Akishita and Tsuyoshi Takagi</i>	
On the Security of Multiple Encryption or CCA-security+CCA-security=CCA-security? . . . . .	360
<i>Rui Zhang, Goichiro Hanaoka, Junji Shikata, and Hideki Imai</i>	
QuasiModo: Efficient Certificate Validation and Revocation . . . . .	375
<i>Farid F. Elwailly, Craig Gentry, and Zulfikar Ramzan</i>	

A Distributed Online Certificate Status Protocol with a Single Public Key .....	389
<i>Satoshi Koga and Kouichi Sakurai</i>	
A First Approach to Provide Anonymity in Attribute Certificates .....	402
<i>Vicente Benjumea, Javier Lopez, Jose A. Montenegro, and Jose M. Troya</i>	
A Nonuniform Algorithm for the Hidden Number Problem in Subgroups .....	416
<i>Igor E. Shparlinski and Arne Winterhof</i>	
Cryptographic Randomized Response Techniques .....	425
<i>Andris Ambainis, Markus Jakobsson, and Helger Lipmaa</i>	
A Correct, Private, and Efficient Mix Network .....	439
<i>Kun Peng, Colin Boyd, Ed Dawson, and Kapali Viswanathan</i>	
<b>Author Index</b> .....	455

Public Key Cryptography -- PKC 2004

7th International Workshop on Theory and Practice in

Public Key Cryptography, Singapore, March 1-4, 2004

Bao, F.; Deng, R.; Zhou, J. (Eds.)

2004, XIII, 459 p., Softcover

ISBN: 978-3-540-21018-4