

Table of Contents

Public Key Cryptography I

Chosen-Ciphertext Security without Redundancy	1
<i>Duong Hieu Phan and David Pointcheval</i>	
Some RSA-Based Encryption Schemes with Tight Security Reduction	19
<i>Kaoru Kurosawa and Tsuyoshi Takagi</i>	
A Simple Public-Key Cryptosystem with a Double Trapdoor Decryption Mechanism and Its Applications	37
<i>Emmanuel Bresson, Dario Catalano, and David Pointcheval</i>	

Number Theory I

Factoring Estimates for a 1024-Bit RSA Modulus	55
<i>Arjen Lenstra, Eran Tromer, Adi Shamir, Wil Kortsmit, Bruce Dodson, James Hughes, and Paul Leyland</i>	
Index Calculus Attack for Hyperelliptic Curves of Small Genus	75
<i>Nicolas Thériault</i>	

Efficient Implementations

Parallelizing Explicit Formula for Arithmetic in the Jacobian of Hyperelliptic Curves	93
<i>Pradeep Kumar Mishra and Palash Sarkar</i>	
Tate Pairing Implementation for Hyperelliptic Curves $y^2 = x^p - x + d$	111
<i>Iwan Duursma and Hyang-Sook Lee</i>	
The AGM- $X_0(N)$ Heegner Point Lifting Algorithm and Elliptic Curve Point Counting	124
<i>David R. Kohel</i>	

Key Management and Protocols

Key Management Schemes for Stateless Receivers Based on Time Varying Heterogeneous Logical Key Hierarchy	137
<i>Miodrag J. Mihaljević</i>	
Leakage-Resilient Authenticated Key Establishment Protocols	155
<i>SeongHan Shin, Kazukuni Kobara, and Hideki Imai</i>	
Untraceable Fair Network Payment Protocols with Off-Line TTP	173
<i>Chih-Hung Wang</i>	

Hash Functions

Incremental Multiset Hash Functions and Their Application to Memory Integrity Checking	188
<i>Dwayne Clarke, Srinivas Devadas, Marten van Dijk, Blaise Gassend, and G. Edward Suh</i>	
New Parallel Domain Extenders for UOWHF	208
<i>Wonil Lee, Donghoon Chang, Sangjin Lee, Soohak Sung, and Mridul Nandi</i>	
Cryptanalysis of 3-Pass HAVAL	228
<i>Bart Van Rompay, Alex Biryukov, Bart Preneel, and Joos Vandewalle</i>	

Group Signatures

Efficient Group Signatures without Trapdoors	246
<i>Giuseppe Ateniese and Breno de Medeiros</i>	
Accumulating Composites and Improved Group Signing	269
<i>Gene Tsudik and Shouhua Xu</i>	
Almost Uniform Density of Power Residues and the Provable Security of ESIGN	287
<i>Tatsuaki Okamoto and Jacques Stern</i>	

Number Theory II

Rotations and Translations of Number Field Sieve Polynomials	302
<i>Jason E. Gower</i>	
On Class Group Computations Using the Number Field Sieve	311
<i>Mark L. Bauer and Safuat Hamdy</i>	

Invited Talk

The Secret and Beauty of Ancient Chinese Padlocks	326
<i>Hong-Sen Yan and Hsing-Hui Huang</i>	

Block Ciphers

A Traceable Block Cipher	331
<i>Olivier Billet and Henri Gilbert</i>	
A New Attack against Khazad	347
<i>Frédéric Muller</i>	

Broadcast and Multicast

An Efficient Public Key Trace and Revoke Scheme Secure against Adaptive Chosen Ciphertext Attack	359
<i>Chong Hee Kim, Yong Ho Hwang, and Pil Joong Lee</i>	

Sequential Key Derivation Patterns for Broadcast Encryption and Key Predistribution Schemes	374
<i>Nuttapong Attrapadung, Kazukuni Kobara, and Hideki Imai</i>	

Foundations and Complexity Theory

Boneh <i>et al.</i> 's k -Element Aggregate Extraction Assumption Is Equivalent to the Diffie-Hellman Assumption	392
<i>Jean-Sebastien Coron and David Naccache</i>	

On Diophantine Complexity and Statistical Zero-Knowledge Arguments ..	398
<i>Helger Lipmaa</i>	

Verifiable Homomorphic Oblivious Transfer and Private Equality Test	416
<i>Helger Lipmaa</i>	

Public Key Cryptography II

Generalized Powering Functions and Their Application to Digital Signatures	434
<i>Hisayoshi Sato, Tsuyoshi Takagi, Satoru Tezuka, and Kazuo Takaragi</i>	

Certificateless Public Key Cryptography	452
<i>Sattam S. Al-Riyami and Kenneth G. Paterson</i>	

A Complete and Explicit Security Reduction Algorithm for RSA-Based Cryptosystems	474
<i>Kaoru Kurosawa, Katja Schmidt-Samoa, and Tsuyoshi Takagi</i>	

The Insecurity of Esign in Practical Implementations	492
<i>Pierre-Alain Fouque, Nick Howgrave-Graham, Gwenaëlle Martinet, and Guillaume Poupard</i>	

Digital Signature

Efficient One-Time Proxy Signatures	507
<i>Huaxiong Wang and Josef Pieprzyk</i>	

Universal Designated-Verifier Signatures	523
<i>Ron Steinfeld, Laurence Bull, Huaxiong Wang, and Josef Pieprzyk</i>	

Author Index	543
--------------------	-----

Advances in Cryptology - ASIACRYPT 2003
9th International Conference on the Theory and
Application of Cryptology and Information Security,
Taipei, Taiwan, November 30 - December 4, 2003,
Proceedings
Laih, C.S. (Ed.)
2003, XIV, 550 p., Softcover
ISBN: 978-3-540-20592-0