

Table of Contents

Lattice Based Cryptography

Cryptanalysis of the NTRU Signature Scheme (NSS) from Eurocrypt 2001	1
<i>Craig Gentry, Jakob Jonsson, Jacques Stern, Michael Szydlo</i>	
On the Insecurity of a Server-Aided RSA Protocol	21
<i>Phong Q. Nguyen, Igor E. Shparlinski</i>	
The Modular Inversion Hidden Number Problem	36
<i>Dan Boneh, Shai Halevi, Nick Howgrave-Graham</i>	

Human Identification

Secure Human Identification Protocols	52
<i>Nicholas J. Hopper, Manuel Blum</i>	

Invited Talk

Unbelievable Security (<i>Matching AES Security Using Public Key Systems</i>)	67
<i>Arjen K. Lenstra</i>	

Practical Public Key Cryptography

A Probable Prime Test with Very High Confidence for $n \equiv 1 \pmod{4}$	87
<i>Siguna Müller</i>	
Computation of Discrete Logarithms in $\mathbb{F}_{2^{607}}$	107
<i>Emmanuel Thomé</i>	
Speeding Up XTR	125
<i>Martijn Stam, Arjen K. Lenstra</i>	
An Efficient Implementation of Braid Groups	144
<i>Jae Choon Cha, Ki Hyoung Ko, Sang Jin Lee, Jae Woo Han, Jung Hee Cheon</i>	

Cryptography Based on Coding Theory

How to Achieve a McEliece-Based Digital Signature Scheme	157
<i>Nicolas T. Courtois, Matthieu Finiasz, Nicolas Sendrier</i>	
Efficient Traitor Tracing Algorithms Using List Decoding	175
<i>Alice Silverberg, Jessica Staddon, Judy L. Walker</i>	

Block Ciphers

Security of Reduced Version of the Block Cipher Camellia against Truncated and Impossible Differential Cryptanalysis	193
<i>Makoto Sugita, Kazukuni Kobara, Hideki Imai</i>	
Known-IV Attacks on Triple Modes of Operation of Block Ciphers	208
<i>Deukjo Hong, Jaechul Sung, Seokhie Hong, Wonil Lee, Sangjin Lee, Jongin Lim, Okyeon Yi</i>	
Generic Attacks on Feistel Schemes	222
<i>Jacques Patarin</i>	
A Compact Rijndael Hardware Architecture with S-Box Optimization	239
<i>Akashi Satoh, Sumio Morioka, Kohji Takano, Seiji Munetoh</i>	

Provable Security

Provable Security of KASUMI and 3GPP Encryption Mode f_8	255
<i>Ju-Sung Kang, Sang-Uk Shin, Dowon Hong, Okyeon Yi</i>	
Efficient and Mutually Authenticated Key Exchange for Low Power Computing Devices	272
<i>Duncan S. Wong, Agnes H. Chan</i>	
Provably Authenticated Group Diffie-Hellman Key Exchange – The Dynamic Case	290
<i>Emmanuel Bresson, Olivier Chevassut, David Pointcheval</i>	

Threshold Cryptography

Fully Distributed Threshold RSA under Standard Assumptions	310
<i>Pierre-Alain Fouque, Jacques Stern</i>	
Adaptive Security in the Threshold Setting: From Cryptosystems to Signature Schemes	331
<i>Anna Lysyanskaya, Chris Peikert</i>	
Threshold Cryptosystems Secure against Chosen-Ciphertext Attacks	351
<i>Pierre-Alain Fouque, David Pointcheval</i>	

Two-Party Protocols

Oblivious Polynomial Evaluation and Oblivious Neural Learning	369
<i>Yan-Cheng Chang, Chi-Jen Lu</i>	
Mutually Independent Commitments	385
<i>Moses Liskov, Anna Lysyanskaya, Silvio Micali, Leonid Reyzin, Adam Smith</i>	

Zero Knowledge

Efficient Zero-Knowledge Authentication Based on a Linear Algebra Problem MinRank.....	402
<i>Nicolas T. Courtois</i>	

Responsive Round Complexity and Concurrent Zero-Knowledge.....	422
<i>Tzafirir Cohen, Joe Kilian, Erez Petrank</i>	

Cryptographic Building Blocks

Practical Construction and Analysis of Pseudo-Randomness Primitives ...	442
<i>Johan Håstad, Mats Näslund</i>	

Autocorrelation Coefficients and Correlation Immunity of Boolean Functions	460
<i>Yuriy Tarannikov, Peter Korolev, Anton Botev</i>	

Elliptic Curve Cryptography

An Extension of Kedlaya's Point-Counting Algorithm to Superelliptic Curves	480
<i>Pierrick Gaudry, Nicolas Gürel</i>	

Supersingular Curves in Cryptography.....	495
<i>Steven D. Galbraith</i>	

Short Signatures from the Weil Pairing	514
<i>Dan Boneh, Ben Lynn, Hovav Shacham</i>	

Self-Blindable Credential Certificates from the Weil Pairing	533
<i>Eric R. Verheul</i>	

Anonymity

How to Leak a Secret.....	552
<i>Ronald L. Rivest, Adi Shamir, Yael Tauman</i>	

Key-Privacy in Public-Key Encryption.....	566
<i>Mihir Bellare, Alexandra Boldyreva, Anand Desai, David Pointcheval</i>	

Provably Secure Fair Blind Signatures with Tight Revocation.....	583
<i>Masayuki Abe, Miyako Ohkubo</i>	

Author Index	603
---------------------------	-----

Advances in Cryptology — ASIACRYPT 2001
7th International Conference on the Theory and
Application of Cryptology and Information Security Gold
Coast, Australia, December 9-13, 2001. Proceedings
Boyd, C. (Ed.)
2001, XI, 601 p. 22 illus., Softcover
ISBN: 978-3-540-42987-6