

Table of Contents

Invited Talk

Modulus Search for Elliptic Curve Cryptosystems	1
<i>K. Koyama, Y. Tsuruoka, N. Kunihiro</i>	

Asymmetric Key Cryptosystems

On the Lai-Massey Scheme	8
<i>S. Vaudenay</i>	
On Cryptographically Secure Vectorial Boolean Functions	20
<i>T. Satoh, T. Iwata, K. Kurosawa</i>	

Analysis

Equivalent Keys of HPC	29
<i>C. D'Halluin, G. Bijnens, B. Preneel, V. Rijmen</i>	
Cryptanalysis of Five Rounds of CRYPTON Using Impossible Differentials	43
<i>H. Seki, T. Kaneko</i>	
Cryptanalysis of Two Cryptosystems Based on Group Actions	52
<i>S. R. Blackburn, S. D. Galbraith</i>	
Probabilistic Higher Order Differential Attack and Higher Order Bent Functions	62
<i>T. Iwata, K. Kurosawa</i>	

Elliptic Curve Cryptosystems

Fast Algorithms for Elliptic Curve Cryptosystems over Binary Finite Field	75
<i>Y. F. Han, P.-C. Leong, P.-C. Tan, J. Zhang</i>	
Optimizing the Menezes-Okamoto-Vanstone (MOV) Algorithm for Non-supersingular Elliptic Curves	86
<i>J. Shikata, Y. Zheng, J. Suzuki, H. Imai</i>	
Speeding up the Discrete Log Computation on Curves with Automorphisms	103
<i>I. Duursma, P. Gaudry, F. Morain</i>	
ECC: Do We Need to Count?	122
<i>J.-S. Coron, H. Handschuh, D. Naccache</i>	
Elliptic Scalar Multiplication Using Point Halving	135
<i>E. W. Knudsen</i>	

Public Key Cryptosystems

On the Design of RSA with Short Secret Exponent	150
<i>H.-M. Sun, W.-C. Yang, C.-S. Lai</i>	
Efficient Public-Key Cryptosystems Provably Secure Against Active Adversaries	165
<i>P. Paillier, D. Pointcheval</i>	
Adaptively-Secure Optimal-Resilience Proactive RSA	180
<i>Y. Frankel, P. MacKenzie, M. Yung</i>	

Integers and Computation

Factorization of RSA-140 Using the Number Field Sieve	195
<i>S. Cavallar, B. Dodson, A. Lenstra, P. Leyland, W. Lioen, P. L. Montgomery, B. Murphy, H. te Riele, P. Zimmermann</i>	
How to Prove that a Committed Number Is Prime	208
<i>T. V. Le, K. Q. Nguyen, V. Varadharajan</i>	
Reducing Logarithms in Totally Non-maximal Imaginary Quadratic Orders to Logarithms in Finite Fields	219
<i>D. Hühnlein, T. Takagi</i>	
General Adversaries in Unconditional Multi-party Computation	232
<i>M. Fitzi, M. Hirt, U. Maurer</i>	

Network Security

Approximation Hardness and Secure Communication in Broadcast Channels	247
<i>Y. Desmedt, Y. Wang</i>	
Mix-Networks on Permutation Networks	258
<i>M. Abe</i>	
Secure Communication in an Unknown Network Using Certificates	274
<i>M. Burmester, Y. Desmedt</i>	

Random Number

Linear Complexity versus Pseudorandomness: On Beth and Dai's Result .	288
<i>Y. Wang</i>	
A Class of Explicit Perfect Multi-sequences	299
<i>C. P. Xing, K. Y. Lam, Z. H. Wei</i>	
Cryptanalysis of LFSR-Encrypted Codes with Unknown Combining Function	306
<i>S. Palit, B. K. Roy</i>	

Key Management

Doing More with Fewer Bits	321
<i>A. E. Brouwer, R. Pellikaan, E. R. Verheul</i>	
A Quick Group Key Distribution Scheme with “Entity Revocation”	333
<i>J. Anzai, N. Matsuzaki, T. Matsumoto</i>	
An Efficient Hierarchical Identity-Based Key-Sharing Method Resistant Against Collusion-Attacks	348
<i>G. Hanaoka, T. Nishioaka, Y. Zheng, H. Imai</i>	
Periodical Multi-secret Threshold Cryptosystems	363
<i>M. Numao</i>	

Authentication

A Signature Scheme with Message Recovery as Secure as Discrete Logarithm	378
<i>M. Abe, T. Okamoto</i>	
A^3 -codes Under Collusion Attacks	390
<i>Y. J. Wang, R. Safavi-Naini</i>	
Broadcast Authentication in Group Communication	399
<i>R. Safavi-Naini, H. X. Wang</i>	

Author Index	413
---------------------------	-----

Advances in Cryptology - ASIACRYPT'99
International Conference on the Theory and Application
of Cryptology and Information Security, Singapore,
November 14-18, 1999 Proceedings
Lam, K.Y.; Okamoto, E.; Xing, C. (Eds.)
1999, XII, 420 p., Softcover
ISBN: 978-3-540-66666-0