

Table of Contents

Key Self-protection

Forward-Security in Private-Key Cryptography	1
<i>Mihir Bellare and Bennet Yee</i>	
Intrusion-Resilient Public-Key Encryption	19
<i>Yevgeniy Dodis, Matt Franklin, Jonathan Katz, Atsuko Miyaji, and Moti Yung</i>	

Message Authentication

TMAC: Two-Key CBC MAC	33
<i>Kaoru Kurosawa and Tetsu Iwata</i>	
Montgomery Prime Hashing for Message Authentication	50
<i>Douglas L. Whiting and Michael J. Sabin</i>	

Digital Signatures

An Analysis of Proxy Signatures: Is a Secure Channel Necessary?	68
<i>Jung-Yeun Lee, Jung Hee Cheon, and Seungjoo Kim</i>	
Invisibility and Anonymity of Undeniable and Confirmer Signatures	80
<i>Steven D. Galbraith and Wenbo Mao</i>	

Pairing Based Cryptography

A Secure Signature Scheme from Bilinear Maps	98
<i>Dan Boneh, Ilya Mironov, and Victor Shoup</i>	
Access Control Using Pairing Based Cryptography	111
<i>Nigel P. Smart</i>	

Multivariate and Lattice Problems

NTRUSIGN: Digital Signatures Using the NTRU Lattice	122
<i>Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H. Silverman, and William Whyte</i>	
About the XL Algorithm over $GF(2)$	141
<i>Nicolas T. Courtois and Jacques Patarin</i>	

Cryptographic Architectures

Efficient $GF(p^m)$ Arithmetic Architectures
for Cryptographic Applications 158
*Guido Bertoni, Jorge Guajardo, Sandeep Kumar, Gerardo Orlando,
Christof Paar, and Thomas Wollinger*

Hardware Performance Characterization of Block Cipher Structures 176
Lu Xiao and Howard M. Heys

New RSA-based Cryptosystems

Simple Identity-Based Cryptography with Mediated RSA 193
Xuhua Ding and Gene Tsudik

Two Birds One Stone: Signcryption Using RSA 211
John Malone-Lee and Wenbo Mao

Invited Talk I

Cryptography after the Bubble: How to Make an Impact on the World 226
Tom Berson

Chosen-Ciphertext Security

Rethinking Chosen-Ciphertext Security under Kerckhoffs' Assumption 227
Seungjoo Kim, Masahiro Mambo, and Yuliang Zheng

Provably Secure Public-Key Encryption
for Length-Preserving Chaumian Mixes 244
Bodo Möller

Broadcast Encryption and PRF Sharing

Fault Tolerant and Distributed Broadcast Encryption 263
Paolo D'Arco and Douglas R. Stinson

Shared Generation of Pseudo-Random Functions with Cumulative Maps .. 281
Huaxiong Wang and Josef Pieprzyk

Authentication Structures

Authenticated Data Structures for Graph and Geometric Searching 295
*Michael T. Goodrich, Roberto Tamassia, Nikos Triandopoulos,
and Robert Cohen*

Fractal Merkle Tree Representation and Traversal 314
Markus Jakobsson, Tom Leighton, Silvio Micali, and Michael Szydlo

Invited Talk II

RSA Shortcuts	327
<i>Adi Shamir</i>	

Elliptic Curves and Pairings

The Width- w NAF Method Provides Small Memory and Fast Elliptic Scalar Multiplications Secure against Side Channel Attacks	328
<i>Katsuyuki Okeya and Tsuyoshi Takagi</i>	
Fast Elliptic Curve Arithmetic and Improved Weil Pairing Evaluation	343
<i>Kirsten Eisenträger, Kristin Lauter, and Peter L. Montgomery</i>	

Threshold Cryptography

Two Efficient and Provably Secure Schemes for Server-Assisted Threshold Signatures	355
<i>Shouhuai Xu and Ravi Sandhu</i>	
Secure Applications of Pedersen's Distributed Key Generation Protocol ...	373
<i>Rosario Gennaro, Stanisław Jarecki, Hugo Krawczyk, and Tal Rabin</i>	

Implementation Issues

Seeing through MIST Given a Small Fraction of an RSA Private Key	391
<i>Colin D. Walter</i>	
Simple Backdoors for RSA Key Generation	403
<i>Claude Crépeau and Alain Slakmon</i>	
Author Index	417

<http://www.springer.com/978-3-540-00847-7>

Topics in Cryptology -- CT-RSA 2003

The Cryptographers' Track at the RSA Conference

2003, San Francisco, CA, USA April 13-17, 2003,

Proceedings

Joye, M. (Ed.)

2003, XII, 424 p., Softcover

ISBN: 978-3-540-00847-7