Table of Contents

**Key Self-protection**

Forward-Security in Private-Key Cryptography .................................1
*Mihir Bellare and Bennet Yee*

Intrusion-Resilient Public-Key Encryption ................................. 19
*Yevgeniy Dodis, Matt Franklin, Jonathan Katz, Atsuko Miyaji, and Moti Yung*

**Message Authentication**

TMAC: Two-Key CBC MAC ..............................................33
*Kaoru Kurosawa and Tetsu Iwata*

Montgomery Prime Hashing for Message Authentication ............... 50
*Douglas L. Whiting and Michael J. Sabin*

**Digital Signatures**

An Analysis of Proxy Signatures: Is a Secure Channel Necessary? .........68
*Jung-Yeun Lee, Jung Hee Cheon, and Seungjoo Kim*

Invisibility and Anonymity of Undeniable and Confirmer Signatures ........80
*Steven D. Galbraith and Wenbo Mao*

**Pairing Based Cryptography**

A Secure Signature Scheme from Bilinear Maps ..........................98
*Dan Boneh, Ilya Mironov, and Victor Shoup*

Access Control Using Pairing Based Cryptography ...........................111
*Nigel P. Smart*

**Multivariate and Lattice Problems**

NTRUSIGN: Digital Signatures Using the NTRU Lattice .................. 122
*Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H. Silverman, and William Whyte*

About the XL Algorithm over GF(2) .................................. 141
*Nicolas T. Courtois and Jacques Patarin*
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
Seungjoon 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
Huaziong 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
Adi Shamir

Elliptic Curves and Pairings

The Width-\(w\) NAF Method Provides Small Memory
and Fast Elliptic Scalar Multiplications Secure
against Side Channel Attacks ............................................. 328
Katsuyuki Okeya and Tsuyoshi Takagi

Fast Elliptic Curve Arithmetic and Improved Weil Pairing Evaluation .... 343
Kirsten Eisenträger, Kristin Lauter, and Peter L. Montgomery

Threshold Cryptography

Two Efficient and Provably Secure Schemes
for Server-Assisted Threshold Signatures .............................. 355
Shouhuai Xu and Ravi Sandhu

Secure Applications of Pedersen’s Distributed Key Generation Protocol ... 373
Rosario Gennaro, Stanisław Jarecki, Hugo Krawczyk, and Tal Rabin

Implementation Issues

Seeing through Mist Given a Small Fraction of an RSA Private Key ...... 391
Colin D. Walter

Simple Backdoors for RSA Key Generation .............................. 403
Claude Crépeau and Alain Slakman

Author Index ............................................................... 417