Table of Contents

Chosen-Ciphertext Security

Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1 1
Daniel Bleichenbacher

A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack 13
Ronald Cramer, Victor Shoup

Relations Among Notions of Security for Public-Key Encryption Schemes . 26
Mihir Bellare, Anand Desai, David Pointcheval, Phillip Rogaway

Invited Lecture

Cryptography and the Internet 46
Steven M. Bellovin

Cryptanalysis of Hash Functions and Block Ciphers

Differential Collisions in SHA-0 56
Florent Chabaud, Antoine Joux

From Differential Cryptanalysis to Ciphertext-Only Attacks 72
Alex Biryukov, Eyal Kushilevitz

Distributed Cryptography

A Simplified Approach to Threshold and Proactive RSA 89
Tal Rabin

New Efficient and Secure Protocols for Verifiable Signature Sharing and Other Applications 105
Dario Catalano, Rosario Gennaro

Trading Correctness for Privacy in Unconditional Multi-party Computation 121
Matthias Fitzi, Martin Hirt, Ueli Maurer

Identification and Certification

Fast Digital Identity Revocation 137
William Aiello, Sachin Lodha, Rafail Ostrovsky

Self-Delegation with Controlled Propagation – or – What If You Lose Your Laptop 153
Oded Goldreich, Birgit Pfitzmann, Ronald L. Rivest

Identity Escrow 169
Joe Kilian, Erez Petrank

Block Cipher Design and Analysis

Generalized Birthday Attacks on Unbalanced Feistel Networks 186
Charanjit S. Jutla

Quadratic Relation of S-box and Its Application to the Linear Attack of Full Round DES 200
Takeshi Shimoyama, Toshinobu Kaneko

Cryptanalysis of Block Ciphers with Probabilistic Non-linear Relations of Low Degree 212
Thomas Jakobsen

Algebraic Cryptanalysis

Cryptanalysis of the Ajtai-Dwork Cryptosystem 223
Phong Nguyen, Jacques Stern

Cryptanalysis of the Chor-Rivest Cryptosystem 243
Serge Vaudenay

Cryptanalysis of the Oil & Vinegar Signature Scheme 257
Aviad Kipnis, Adi Shamir

Relations Among Cryptographic Primitives

From Unpredictability to Indistinguishability: A Simple Construction of Pseudo-Random Functions from MACs 267
Moni Naor, Omer Reingold

Many-to-One Trapdoor Functions and their Relation to Public-Key Cryptosystems 283
Mihir Bellare, Shai Halevi, Amit Sahai, Salil Vadhan

IACR Distinguished Lecture

Authentication, Enhanced Security and Error Correcting Codes 299
Yonatan Aumann, Michael O. Rabin

Algebraic Schemes

An Efficient Discrete Log Pseudo Random Generator 304
Sarvar Patel, Ganapathy S. Sundaram

Fast RSA-type Cryptosystem Modulo $p^k q$ 318
Tsuyoshi Takagi

An Elliptic Curve Implementation of the Finite Field Digital Signature Algorithm 327
Neal Koblitz

Quantum Cryptography

Quantum Bit Commitment from a Physical Assumption 338
Louis Salvail

Signatures, Random Functions and Ideal Ciphers

On Concrete Security Treatment of Signatures Derived from Identification 354
Kazuo Ohta, Tatsuaki Okamoto

Building PRFs from PRPs 370
Chris Hall, David Wagner, John Kelsey, Bruce Schneier

Security Amplification by Composition: The Case of Doubly-Iterated, Ideal Ciphers 390
William Aiello, Mihir Bellare, Giovanni Di Crescenzo, Ramarathnam Venkatesan

Zero-Knowledge

On the Existence of 3-Round Zero-Knowledge Protocols 408
Satoshi Hada, Toshiaki Tanaka

Zero-Knowledge Proofs for Finite Field Arithmetic, or: Can Zero-Knowledge Be for Free? 424
Ronald Cramer, Ivan Damgård

Concurrent Zero-Knowledge: Reducing the Need for Timing Constraints . . 442
Cynthia Dwork, Amit Sahai

Implementation

The Solution of McCurley's Discrete Log Challenge 458
Damian Weber, Thomas Denny

Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithms . . 472
Daniel V. Bailey, Christof Paar

Rights Protection

Time-Stamping with Binary Linking Schemes 486
Ahto Buldas, Peeter Laud, Helger Lipmaa, Jan Villemson

Threshold Traitor Tracing 502
Moni Naor, Benny Pinkas

Author Index 519