Table of Contents

Foundations
On the (Im)possibility of Obfuscating Programs ......................... 1
Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich,
Amit Sahai, Salil Vadhan, and Ke Yang
Universally Composable Commitments ..................................... 19
Ran Canetti and Marc Fischlin

Traitor Tracing
Revocation and Tracing Schemes for Stateless Receivers .............. 41
Dalit Naor, Moni Naor, and Jeff Lotspiech
Self Protecting Pirates and Black-Box Traitor Tracing ............... 63
Aggelos Kiayias and Moti Yung

Multi-party Computation
Minimal Complete Primitives for Secure Multi-party Computation ..... 80
Matthias Fitzi, Juan A. Garay, Ueli Maurer, and Rafail Ostrovsky
Robustness for Free in Unconditional Multi-party Computation ...... 101
Martin Hirt and Ueli Maurer
Secure Distributed Linear Algebra in a Constant Number of Rounds . 119
Ronald Cramer and Ivan Damgård

Two-Party Computation
Two-Party Generation of DSA Signatures ................................. 137
Philip Mackenzie and Michael K. Rester
Oblivious Transfer in the Bounded Storage Model ..................... 155
Yan Zong Ding
Parallel Coin-Tossing and Constant-Round Secure Two-Party
Computation ........................................................................... 171
Yehuda Lindell

Elliptic Curves
Faster Point Multiplication on Elliptic Curves with Efficient
Endomorphisms ........................................................................ 190
Robert P. Gallant, Robert J. Lambert, and Scott A. Vanstone
On the Unpredictability of Bits of the Elliptic Curve Diffie-Hellman
Scheme ................................................................................... 201
Dan Boneh and Igor E. Shparlinski
Identity-Based Encryption from the Weil Pairing

Dan Boneh and Matt Franklin

OAEP

A Chosen Ciphertext Attack on RSA Optimal Asymmetric Encryption Padding (OAEP) as Standardized in PKCS #1 v2.0

James Manger

OAEP Reconsidered

Victor Shoup

RSA-OAEP Is Secure under the RSA Assumption

Eisichiro Fujisaki, Tatsuaki Okamoto, David Pointcheval, and Jacques Stern

Simplified OAEP for the RSA and Rabin Functions

Dan Boneh

Encryption and Authentication

Online Ciphers and the Hash-CBC Construction

Mihir Bellare, Alexandra Boldyreva, Lars Knudsen, and Chanathip Namprempre

The Order of Encryption and Authentication for Protecting Communications (or: How Secure Is SSL?)

Hugo Krawczyk

Signature Schemes

Forward-Secure Signatures with Optimal Signing and Verifying

Gene Itkis and Leonid Reyzin

Improved Online/Offline Signature Schemes

Adi Shamir and Yael Tauman

Protocols

An Efficient Scheme for Proving a Shuffle

Jun Furukawa and Kazue Sako

An Identity Escrow Scheme with Appointed Verifiers

Jan Camenisch and Anna Lysyanskaya

Session-Key Generation Using Human Passwords Only

Oded Goldreich and Yehuda Lindell

Cryptanalysis

Cryptanalysis of RSA Signatures with Fixed-Pattern Padding

Eric Brier, Christophe Clavier, Jean-Sébastien Coron, and David Naccache

Correlation Analysis of the Shrinking Generator

Jovan D. Golić
Applications of Groups and Codes

Nonlinear Vector Resilient Functions ........................................... 458
  Jung Hee Cheon

New Public Key Cryptosystem Using Finite Non Abelian Groups .......... 470
  Song-Hun Paeng, Ki-Chan Ha, Jae Heon Kim, Seongtaek Chee,
  and Cheonsik Park

Pseudorandomness from Braid Groups ....................................... 486
  Eonkyung Lee, Sang Jin Lee, and Sang Geun Hahn

Broadcast and Secret Sharing

On the Cost of Reconstructing a Secret, or VSS with Optimal
Reconstruction Phase ............................................................ 503
  Ronald Cramer, Ivan Damgård, and Serge Fehr

Secure and Efficient Asynchronous Broadcast Protocols ............... 524
  Christian Cachin, Klaus Kursawe, Frank Petzold, and Victor Shoup

Soundness and Zero-Knowledge

Soundness in the Public-Key Model .......................................... 542
  Silvio Micali and Leonid Reyzin

Robust Non-interactive Zero Knowledge .................................... 566
  Alfredo De Santis, Giovanni Di Crescenzo, Rafail Ostrovsky,
  Giuseppe Persiano, and Amit Sahai

Author Index ............................................................................ 599
Advances in Cryptology - CRYPTO 2001
21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001,
Proceedings
Kilian, J. (Ed.)
2001, XII, 604 p., Softcover
ISBN: 978-3-540-42456-7