

Table of Contents

Foundations

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

Traitor Tracing

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

Multi-party Computation

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

Two-Party Computation

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

Elliptic Curves

Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms	190
<i>Robert P. Gallant, Robert J. Lambert, and Scott A. Vanstone</i>	
On the Unpredictability of Bits of the Elliptic Curve Diffie–Hellman Scheme	201
<i>Dan Boneh and Igor E. Shparlinski</i>	

Identity-Based Encryption from the Weil Pairing.....	213
<i>Dan Boneh and Matt Franklin</i>	

OAEP

A Chosen Ciphertext Attack on RSA Optimal Asymmetric Encryption Padding (OAEP) as Standardized in PKCS #1 v2.0	230
<i>James Manger</i>	
OAEP Reconsidered	239
<i>Victor Shoup</i>	
RSA–OAEP Is Secure under the RSA Assumption	260
<i>Eiichiro Fujisaki, Tatsuaki Okamoto, David Pointcheval, and Jacques Stern</i>	
Simplified OAEP for the RSA and Rabin Functions	275
<i>Dan Boneh</i>	

Encryption and Authentication

Online Ciphers and the Hash-CBC Construction	292
<i>Mihir Bellare, Alexandra Boldyreva, Lars Knudsen, and Chanathip Namprempre</i>	
The Order of Encryption and Authentication for Protecting Communications (or: How Secure Is SSL?)	310
<i>Hugo Krawczyk</i>	

Signature Schemes

Forward-Secure Signatures with Optimal Signing and Verifying	332
<i>Gene Itkis and Leonid Reyzin</i>	
Improved Online/Offline Signature Schemes	355
<i>Adi Shamir and Yael Tauman</i>	

Protocols

An Efficient Scheme for Proving a Shuffle	368
<i>Jun Furukawa and Kazue Sako</i>	
An Identity Escrow Scheme with Appointed Verifiers	388
<i>Jan Camenisch and Anna Lysyanskaya</i>	
Session-Key Generation Using Human Passwords Only	408
<i>Oded Goldreich and Yehuda Lindell</i>	

Cryptanalysis

Cryptanalysis of RSA Signatures with Fixed-Pattern Padding	433
<i>Eric Brier, Christophe Clavier, Jean-Sébastien Coron, and David Naccache</i>	
Correlation Analysis of the Shrinking Generator	440
<i>Jovan D. Golić</i>	

Applications of Groups and Codes

Nonlinear Vector Resilient Functions.....	458
<i>Jung Hee Cheon</i>	
New Public Key Cryptosystem Using Finite Non Abelian Groups	470
<i>Seong-Hun Paeng, Kil-Chan Ha, Jae Heon Kim, Seongtaek Chee, and Choonsik Park</i>	
Pseudorandomness from Braid Groups	486
<i>Eonkyung Lee, Sang Jin Lee, and Sang Geun Hahn</i>	

Broadcast and Secret Sharing

On the Cost of Reconstructing a Secret, or VSS with Optimal Reconstruction Phase.....	503
<i>Ronald Cramer, Ivan Damgård, and Serge Fehr</i>	
Secure and Efficient Asynchronous Broadcast Protocols	524
<i>Christian Cachin, Klaus Kursawe, Frank Petzold, and Victor Shoup</i>	

Soundness and Zero-Knowledge

Soundness in the Public-Key Model.....	542
<i>Silvio Micali and Leonid Reyzin</i>	
Robust Non-interactive Zero Knowledge	566
<i>Alfredo De Santis, Giovanni Di Crescenzo, Rafail Ostrovsky, Giuseppe Persiano, and Amit Sahai</i>	

Author Index.....	599
-------------------	-----

<http://www.springer.com/978-3-540-42456-7>

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