

# Table of Contents

## Elliptic Curves

A Memory Efficient Version of Satoh's Algorithm .....	1
<i>Frederik Vercauteren (K. U. Leuven, Belgium)</i>	
<i>Bart Preneel (K. U. Leuven, Belgium)</i>	
<i>Joos Vandewalle (K. U. Leuven, Belgium)</i>	
Finding Secure Curves with the Satoh-FGH Algorithm and an Early-Abort Strategy .....	14
<i>Mireille Fouquet (LIX, École polytechnique, France)</i>	
<i>Pierrick Gaudry (LIX, École polytechnique, France)</i>	
<i>Robert Harley (ArgoTech, France)</i>	
How Secure Are Elliptic Curves over Composite Extension Fields? .....	30
<i>Nigel P. Smart (University of Bristol, UK)</i>	

## Commitments

Efficient and Non-interactive Non-malleable Commitment .....	40
<i>Giovanni Di Crescenzo (Telcordia Technologies Inc., USA)</i>	
<i>Jonathan Katz (Telcordia Technologies Inc. and Columbia University, USA)</i>	
<i>Rafail Ostrovsky (Telcordia Technologies Inc., USA)</i>	
<i>Adam Smith (Massachusetts Institute of Technology, USA)</i>	
How to Convert the Flavor of a Quantum Bit Commitment .....	60
<i>Claude Crépeau (McGill University, Canada)</i>	
<i>Frédéric Légaré (Zero-Knowledge Systems Inc., Canada)</i>	
<i>Louis Salvail (BRICS, University of Århus, Denmark)</i>	

## Anonymity

Cryptographic Counters and Applications to Electronic Voting .....	78
<i>Jonathan Katz (Telcordia Technologies Inc. and Columbia University, USA)</i>	
<i>Steven Myers (University of Toronto, Canada)</i>	
<i>Rafail Ostrovsky (Telcordia Technologies Inc., USA)</i>	

An Efficient System for Non-transferable Anonymous Credentials  
with Optional Anonymity Revocation ..... 93  
*Jan Camenisch (IBM Zürich Research Laboratory, Switzerland)*  
*Anna Lysyanskaya (Massachusetts Institute of Technology, USA)*

Priced Oblivious Transfer: How to Sell Digital Goods ..... 119  
*Bill Aiello (AT&T Labs – Research, USA)*  
*Yuval Ishai (DIMACS and AT&T Labs – Research, USA)*  
*Omer Reingold (AT&T Labs – Research, USA)*

**Signatures and Hash Functions**

A Secure Three-Move Blind Signature Scheme  
for Polynomially Many Signatures ..... 136  
*Masayuki Abe (NTT Laboratories, Japan)*

Practical Threshold RSA Signatures without a Trusted Dealer ..... 152  
*Ivan Damgård (BRICS, University of Århus, Denmark)*  
*Maciej Koprowski (BRICS, University of Århus, Denmark)*

Hash Functions: From Merkle-Damgård to Shoup ..... 166  
*Ilya Mironov (Stanford University, USA)*

**XTR and NTRU**

Key Recovery and Message Attacks on NTRU-Composite ..... 182  
*Craig Gentry (DoCoMo Communications Laboratories Inc., USA)*

Evidence that XTR Is More Secure  
than Supersingular Elliptic Curve Cryptosystems ..... 195  
*Eric R. Verheul (PricewaterhouseCoopers, The Netherlands)*

NSS: An NTRU Lattice-Based Signature Scheme ..... 211  
*Jeffrey Hoffstein (NTRU Cryptosystems Inc., USA)*  
*Jill Pipher (NTRU Cryptosystems Inc., USA)*  
*Joseph H. Silverman (NTRU Cryptosystems Inc., USA)*

**Assumptions**

The Bit Security of Paillier’s Encryption Scheme and Its Applications .... 229  
*Dario Catalano (University of Catania, Italy)*  
*Rosario Gennaro (IBM T. J. Watson Research Center, USA)*  
*Nick Howgrave-Graham (IBM T. J. Watson Research Center, USA)*

Assumptions Related to Discrete Logarithms:  
Why Subtleties Make a Real Difference ..... 244  
*Ahmad-Reza Sadeghi (Saarland University, Germany)*  
*Michael Steiner (Saarland University, Germany)*

## Multiparty Protocols

On Adaptive vs. Non-adaptive Security of Multiparty Protocols . . . . .	262
<i>Ran Canetti (IBM T. J. Watson Research Center, USA)</i>	
<i>Ivan Damgård (BRICS, University of Århus, Denmark)</i>	
<i>Stefan Dziembowski (BRICS, University of Århus, Denmark)</i>	
<i>Yuval Ishai (DIMACS and AT&amp;T Labs – Research, USA)</i>	
<i>Tal Malkin (AT&amp;T Labs – Research, USA)</i>	
Multiparty Computation from Threshold Homomorphic Encryption . . . . .	280
<i>Ronald Cramer (BRICS, University of Århus, Denmark)</i>	
<i>Ivan Damgård (BRICS, University of Århus, Denmark)</i>	
<i>Jesper B. Nielsen (BRICS, University of Århus, Denmark)</i>	
On Perfect and Adaptive Security in Exposure-Resilient Cryptography . . . .	301
<i>Yevgeniy Dodis (University of New York, USA)</i>	
<i>Amit Sahai (Princeton University, USA)</i>	
<i>Adam Smith (Massachusetts Institute of Technology, USA)</i>	

## Block Ciphers

Cryptanalysis of Reduced-Round MISTY . . . . .	325
<i>Ulrich Kühn (Dresdner Bank AG, Germany)</i>	
The Rectangle Attack – Rectangling the Serpent . . . . .	340
<i>Eli Biham (Technion, Israel)</i>	
<i>Orr Dunkelman (Technion, Israel)</i>	
<i>Nathan Keller (Technion, Israel)</i>	

## Primitives

Efficient Amplification of the Security of Weak Pseudo-Random Function Generators . . . . .	358
<i>Steven Myers (University of Toronto, Canada)</i>	
Min-round Resettable Zero-Knowledge in the Public-Key Model . . . . .	373
<i>Silvio Micali (Massachusetts Institute of Technology, USA)</i>	
<i>Leonid Reyzin (Massachusetts Institute of Technology, USA)</i>	

## Symmetric Ciphers

Structural Cryptanalysis of SASAS . . . . .	394
<i>Alex Biryukov (The Weizmann Institute, Israel)</i>	
<i>Adi Shamir (The Weizmann Institute, Israel)</i>	
Hyper-bent Functions . . . . .	406
<i>Amr M. Youssef (University of Waterloo, Canada)</i>	
<i>Guang Gong (University of Waterloo, Canada)</i>	

New Method for Upper Bounding  
the Maximum Average Linear Hull Probability for SPNs ..... 420  
*Liam Keliher (Queen's University at Kingston, Canada)*  
*Henk Meijer (Queen's University at Kingston, Canada)*  
*Stafford Tavares (Queen's University at Kingston, Canada)*

**Key Exchange and Multicast**

Lower Bounds for Multicast Message Authentication ..... 437  
*Dan Boneh (Stanford University, USA)*  
*Glenn Durfee (Stanford University, USA)*  
*Matt Franklin (University of California, USA)*

Analysis of Key-Exchange Protocols  
and Their Use for Building Secure Channels ..... 453  
*Ran Canetti (IBM T. J. Watson Research Center, USA)*  
*Hugo Krawczyk (Technion, Israel)*

Efficient Password-Authenticated Key Exchange  
Using Human-Memorable Passwords ..... 475  
*Jonathan Katz (Telcordia Technologies Inc. and Columbia University, USA)*  
*Rafail Ostrovsky (Telcordia Technologies Inc., USA)*  
*Moti Yung (CertCo Inc., USA)*

**Authentication and Identification**

Identification Protocols Secure against Reset Attacks ..... 495  
*Mihir Bellare (University of California at San Diego, USA)*  
*Marc Fischlin (University of Frankfurt, Germany)*  
*Shafi Goldwasser (Massachusetts Institute of Technology, USA)*  
*Silvio Micali (Massachusetts Institute of Technology, USA)*

Does Encryption with Redundancy Provide Authenticity? ..... 512  
*Jee Hea An (University of California at San Diego, USA)*  
*Mihir Bellare (University of California at San Diego, USA)*

Encryption Modes with Almost Free Message Integrity ..... 529  
*Charanjit S. Jutla (IBM T. J. Watson Research Center, USA)*

**Author Index** ..... 545

Advances in Cryptology - EUROCRYPT 2001  
International Conference on the Theory and Application  
of Cryptographic Techniques Innsbruck, Austria, May  
6-10, 2001, Proceedings  
Pfitzmann, B. (Ed.)  
2001, XIII, 544 p. 23 illus., Softcover  
ISBN: 978-3-540-42070-5