

# Table of Contents

## Private Computation

Efficient Private Matching and Set Intersection . . . . .	1
<i>Michael J. Freedman, Kobbi Nissim, and Benny Pinkas</i>	
Positive Results and Techniques for Obfuscation . . . . .	20
<i>Benjamin Lynn, Manoj Prabhakaran, and Amit Sahai</i>	
Secure Computation of the $k^{\text{th}}$ -Ranked Element . . . . .	40
<i>Gagan Aggarwal, Nina Mishra, and Benny Pinkas</i>	

## Signatures I

Short Signatures Without Random Oracles . . . . .	56
<i>Dan Boneh and Xavier Boyen</i>	
Sequential Aggregate Signatures from Trapdoor Permutations . . . . .	74
<i>Anna Lysyanskaya, Silvio Micali, Leonid Reyzin, and Hovav Shacham</i>	

## Unconditional Security

On the Key-Uncertainty of Quantum Ciphers and the Computational Security of One-Way Quantum Transmission . . . . .	91
<i>Ivan Damgård, Thomas Pedersen, and Louis Salvail</i>	
The Exact Price for Unconditionally Secure Asymmetric Cryptography . .	109
<i>Renato Renner and Stefan Wolf</i>	
On Generating the Initial Key in the Bounded-Storage Model . . . . .	126
<i>Stefan Dziembowski and Ueli Maurer</i>	

## Distributed Cryptography

Practical Large-Scale Distributed Key Generation . . . . .	138
<i>John Canny and Stephen Sorkin</i>	
Optimal Communication Complexity of Generic Multicast Key Distribution . . . . .	153
<i>Daniele Micciancio and Saurabh Panjwani</i>	

## Foundations I

An Uninstantiable Random-Oracle-Model Scheme for a Hybrid-Encryption Problem .....	171
<i>Mihir Bellare, Alexandra Boldyreva, and Adriana Palacio</i>	
Black-Box Composition Does Not Imply Adaptive Security .....	189
<i>Steven Myers</i>	

## Identity-Based Encryption

Chosen-Ciphertext Security from Identity-Based Encryption .....	207
<i>Ran Canetti, Shai Halevi, and Jonathan Katz</i>	
Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles .....	223
<i>Dan Boneh and Xavier Boyen</i>	

## Elliptic Curves

Construction of Secure Random Curves of Genus 2 over Prime Fields ....	239
<i>Pierrick Gaudry and Éric Schost</i>	
Projective Coordinates Leak .....	257
<i>David Naccache, Nigel P. Smart, and Jacques Stern</i>	

## Signatures II

Security Proofs for Identity-Based Identification and Signature Schemes ..	268
<i>Mihir Bellare, Chanathip Namprempre, and Gregory Neven</i>	
Concurrent Signatures .....	287
<i>Liqun Chen, Caroline Kudla, and Kenneth G. Paterson</i>	
The Hierarchy of Key Evolving Signatures and a Characterization of Proxy Signatures .....	306
<i>Tal Malkin, Satoshi Obana, and Moti Yung</i>	

## Public-Key Cryptography

Public-Key Steganography .....	323
<i>Luis von Ahn and Nicholas J. Hopper</i>	
Immunizing Encryption Schemes from Decryption Errors .....	342
<i>Cynthia Dwork, Moni Naor, and Omer Reingold</i>	
Secure Hashed Diffie-Hellman over Non-DDH Groups .....	361
<i>Rosario Gennaro, Hugo Krawczyk, and Tal Rabin</i>	

## Foundations II

On Simulation-Sound Trapdoor Commitments .....	382
<i>Philip MacKenzie and Ke Yang</i>	

Hash Function Balance and Its Impact on Birthday Attacks .....	401
<i>Mihir Bellare and Tadayoshi Kohno</i>	

## Multiparty Computation

Multi-party Computation with Hybrid Security .....	419
<i>Matthias Fitzi, Thomas Holenstein, and Jürg Wullschleger</i>	

On the Hardness of Information-Theoretic Multiparty Computation .....	439
<i>Yuval Ishai and Eyal Kushilevitz</i>	

Dining Cryptographers Revisited .....	456
<i>Philippe Golle and Ari Juels</i>	

## Cryptanalysis

Algebraic Attacks and Decomposition of Boolean Functions .....	474
<i>Willi Meier, Enes Pasalic, and Claude Carlet</i>	

Finding Small Roots of Bivariate Integer Polynomial Equations Revisited .....	492
<i>Jean-Sébastien Coron</i>	

## New Applications

Public Key Encryption with Keyword Search .....	506
<i>Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano</i>	

Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data .....	523
<i>Yevgeniy Dodis, Leonid Reyzin, and Adam Smith</i>	

## Algorithms and Implementation

Merkle Tree Traversal in Log Space and Time .....	541
<i>Michael Szydło</i>	

Can We Trust Cryptographic Software? Cryptographic Flaws in GNU Privacy Guard v1.2.3 .....	555
<i>Phong Q. Nguyen</i>	

## **Anonymity**

Traceable Signatures .....	571
<i>Aggelos Kiayias, Yiannis Tsiounis, and Moti Yung</i>	
Handcuffing Big Brother: an Abuse-Resilient Transaction Escrow Scheme .....	590
<i>Stanislaw Jarecki and Vitaly Shmatikov</i>	
Anonymous Identification in <i>Ad Hoc</i> Groups .....	609
<i>Yevgeniy Dodis, Aggelos Kiayias, Antonio Nicolosi, and Victor Shoup</i>	
<b>Author Index</b> .....	627

Advances in Cryptology - EUROCRYPT 2004  
International Conference on the Theory and  
Applications of Cryptographic Techniques, Interlaken,  
Switzerland, May 2-6, 2004. Proceedings  
Cachin, C.; Camensich, J. (Eds.)  
2004, XII, 630 p., Softcover  
ISBN: 978-3-540-21935-4