

# Table of Contents

## Linear Cryptanalysis

On Multiple Linear Approximations . . . . .	1
<i>Alex Biryukov, Christophe De Cannière, and Michaël Quisquater</i>	
Feistel Schemes and Bi-linear Cryptanalysis . . . . .	23
<i>Nicolas T. Courtois</i>	

## Group Signatures

Short Group Signatures . . . . .	41
<i>Dan Boneh, Xavier Boyen, and Hovav Shacham</i>	
Signature Schemes and Anonymous Credentials from Bilinear Maps . . . . .	56
<i>Jan Camenisch and Anna Lysyanskaya</i>	

## Foundations

Complete Classification of Bilinear Hard-Core Functions . . . . .	73
<i>Thomas Holenstein, Ueli Maurer, and Johan Sjödin</i>	
Finding Collisions on a Public Road, or Do Secure Hash Functions Need Secret Coins? . . . . .	92
<i>Chun-Yuan Hsiao and Leonid Reyzin</i>	
Security of Random Feistel Schemes with 5 or More Rounds . . . . .	106
<i>Jacques Patarin</i>	

## Efficient Representations

Signed Binary Representations Revisited . . . . .	123
<i>Katsuyuki Okeya, Katja Schmidt-Samoa, Christian Spahn, and Tsuyoshi Takagi</i>	
Compressed Pairings . . . . .	140
<i>Michael Scott and Paulo S.L.M. Barreto</i>	
Asymptotically Optimal Communication for Torus-Based Cryptography . .	157
<i>Marten van Dijk and David Woodruff</i>	
How to Compress Rabin Ciphertexts and Signatures (and More) . . . . .	179
<i>Craig Gentry</i>	

**Public Key Cryptanalysis**

On the Bounded Sum-of-Digits Discrete Logarithm Problem  
in Finite Fields ..... 201  
*Qi Cheng*

Computing the RSA Secret Key Is Deterministic Polynomial Time  
Equivalent to Factoring ..... 213  
*Alexander May*

**Zero-Knowledge**

Multi-trapdoor Commitments and Their Applications to Proofs  
of Knowledge Secure Under Concurrent Man-in-the-Middle Attacks ..... 220  
*Rosario Gennaro*

Constant-Round Resettable Zero Knowledge  
with Concurrent Soundness in the Bare Public-Key Model ..... 237  
*Giovanni Di Crescenzo, Giuseppe Persiano, and Ivan Visconti*

Zero-Knowledge Proofs  
and String Commitments Withstanding Quantum Attacks ..... 254  
*Ivan Damgård, Serge Fehr, and Louis Salvail*

The Knowledge-of-Exponent Assumptions  
and 3-Round Zero-Knowledge Protocols ..... 273  
*Mihir Bellare and Adriana Palacio*

**Hash Collisions**

Near-Collisions of SHA-0 ..... 290  
*Eli Biham and Rafi Chen*

Multicollisions in Iterated Hash Functions.  
Application to Cascaded Constructions ..... 306  
*Antoine Joux*

**Secure Computation**

Adaptively Secure Feldman VSS and Applications  
to Universally-Composable Threshold Cryptography ..... 317  
*Masayuki Abe and Serge Fehr*

Round-Optimal Secure Two-Party Computation ..... 335  
*Jonathan Katz and Rafail Ostrovsky*

**Invited Talk**

Security, Liberty, and Electronic Communications ..... 355  
*Susan Landau*

## Stream Cipher Cryptanalysis

An Improved Correlation Attack Against Irregular Clocked and Filtered Keystream Generators .....	373
<i>Håvard Molland and Tor Helleseeth</i>	

Rewriting Variables: The Complexity of Fast Algebraic Attacks on Stream Ciphers .....	390
<i>Philip Hawkes and Gregory G. Rose</i>	

Faster Correlation Attack on Bluetooth Keystream Generator E0 .....	407
<i>Yi Lu and Serge Vaudenay</i>	

## Public Key Encryption

A New Paradigm of Hybrid Encryption Scheme .....	426
<i>Kaoru Kurosawa and Yvo Desmedt</i>	

Secure Identity Based Encryption Without Random Oracles .....	443
<i>Dan Boneh and Xavier Boyen</i>	

## Bounded Storage Model

Non-interactive Timestamping in the Bounded Storage Model .....	460
<i>Tal Moran, Ronen Shaltiel, and Amnon Ta-Shma</i>	

## Key Management

IPAKE: Isomorphisms for Password-Based Authenticated Key Exchange ...	477
<i>Dario Catalano, David Pointcheval, and Thomas Pornin</i>	

Randomness Extraction and Key Derivation Using the CBC, Cascade and HMAC Modes .....	494
<i>Yevgeniy Dodis, Rosario Gennaro, Johan Håstad, Hugo Krawczyk, and Tal Rabin</i>	

Efficient Tree-Based Revocation in Groups of Low-State Devices .....	511
<i>Michael T. Goodrich, Jonathan Z. Sun, and Roberto Tamassia</i>	

## Computationally Unbounded Adversaries

Privacy-Preserving Datamining on Vertically Partitioned Databases .....	528
<i>Cynthia Dwork and Kobbi Nissim</i>	

Optimal Perfectly Secure Message Transmission .....	545
<i>K. Srinathan, Arvind Narayanan, and C. Pandu Rangan</i>	

Pseudo-signatures, Broadcast, and Multi-party Computation from Correlated Randomness .....	562
<i>Matthias Fitzi, Stefan Wolf, and Jürg Wullschlegler</i>	

Author Index .....	579
--------------------	-----

Advances in Cryptology - CRYPTO 2004

24th Annual International Cryptology Conference, Santa  
Barbara, California, USA, August 15-19, 2004,

Proceedings

Franklin, M. (Ed.)

2004, XI, 582 p., Softcover

ISBN: 978-3-540-22668-0