

Table of Contents

Public Key Cryptanalysis I

Factoring Large Numbers with the TWIRL Device	1
<i>Adi Shamir, Eran Tromer</i>	
New Partial Key Exposure Attacks on RSA	27
<i>Johannes Blömer, Alexander May</i>	
Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases	44
<i>Jean-Charles Faugère, Antoine Joux</i>	

Alternate Adversary Models

On Constructing Locally Computable Extractors and Cryptosystems in the Bounded Storage Model	61
<i>Salil P. Vadhan</i>	
Unconditional Authenticity and Privacy from an Arbitrarily Weak Secret	78
<i>Renato Renner, Stefan Wolf</i>	

Invited Talk I

On Cryptographic Assumptions and Challenges	96
<i>Moni Naor</i>	

Protocols

Scalable Protocols for Authenticated Group Key Exchange	110
<i>Jonathan Katz, Moti Yung</i>	
Practical Verifiable Encryption and Decryption of Discrete Logarithms	126
<i>Jan Camenisch, Victor Shoup</i>	
Extending Oblivious Transfers Efficiently	145
<i>Yuval Ishai, Joe Kilian, Kobbi Nissim, Erez Petrank</i>	

Symmetric Key Cryptanalysis I

Algebraic Attacks on Combiners with Memory	162
<i>Frederik Armknecht, Matthias Krause</i>	

Fast Algebraic Attacks on Stream Ciphers with Linear Feedback	176
<i>Nicolas T. Courtois</i>	

Cryptanalysis of SAFER++	195
<i>Alex Biryukov, Christophe De Cannière, Gustaf Dellkrantz</i>	

Public Key Cryptanalysis II

A Polynomial Time Algorithm for the Braid Diffie-Hellman Conjugacy Problem	212
<i>Jung Hee Cheon, Byungheup Jun</i>	

The Impact of Decryption Failures on the Security of NTRU Encryption	226
<i>Nick Howgrave-Graham, Phong Q. Nguyen, David Pointcheval, John Proos, Joseph H. Silverman, Ari Singer, William Whyte</i>	

Universal Composability

Universally Composable Efficient Multiparty Computation from Threshold Homomorphic Encryption	247
<i>Ivan Damgård, Jesper Buus Nielsen</i>	

Universal Composition with Joint State	265
<i>Ran Canetti, Tal Rabin</i>	

Zero-Knowledge

Statistical Zero-Knowledge Proofs with Efficient Provers: Lattice Problems and More	282
<i>Daniele Micciancio, Salil P. Vadhan</i>	

Derandomization in Cryptography	299
<i>Boaz Barak, Shien Jin Ong, Salil P. Vadhan</i>	

On Deniability in the Common Reference String and Random Oracle Model	316
<i>Rafael Pass</i>	

Algebraic Geometry

Primality Proving via One Round in ECPP and One Iteration in AKS	338
<i>Qi Cheng</i>	

Torus-Based Cryptography	349
<i>Karl Rubin, Alice Silverberg</i>	

Public Key Constructions

Efficient Universal Padding Techniques for Multiplicative Trapdoor One-Way Permutation	366
<i>Yuichi Komano, Kazuo Ohta</i>	
Multipurpose Identity-Based Signcryption (A Swiss Army Knife for Identity-Based Cryptography)	383
<i>Xavier Boyen</i>	

Invited Talk II

SIGMA: The ‘SIGn-and-MAC’ Approach to Authenticated Diffie-Hellman and Its Use in the IKE Protocols	400
<i>Hugo Krawczyk</i>	

New Problems

On Memory-Bound Functions for Fighting Spam	426
<i>Cynthia Dwork, Andrew Goldberg, Moni Naor</i>	
Lower and Upper Bounds on Obtaining History Independence	445
<i>Niv Buchbinder, Erez Petrank</i>	
Private Circuits: Securing Hardware against Probing Attacks	463
<i>Yuval Ishai, Amit Sahai, David Wagner</i>	

Symmetric Key Constructions

A Tweakable Enciphering Mode	482
<i>Shai Halevi, Phillip Rogaway</i>	
A Message Authentication Code Based on Unimodular Matrix Groups ...	500
<i>Matthew Cary, Ramarathnam Venkatesan</i>	
Luby-Rackoff: 7 Rounds Are Enough for $2^{n(1-\epsilon)}$ Security	513
<i>Jacques Patarin</i>	

New Models

Weak Key Authenticity and the Computational Completeness of Formal Encryption	530
<i>Omer Horvitz, Virgil Gligor</i>	
Plaintext Awareness via Key Registration	548
<i>Jonathan Herzog, Moses Liskov, Silvio Micali</i>	
Relaxing Chosen-Ciphertext Security	565
<i>Ran Canetti, Hugo Krawczyk, Jesper Buus Nielsen</i>	

Symmetric Key Cryptanalysis II

Password Interception in a SSL/TLS Channel 583
 Brice Canvel, Alain Hiltgen, Serge Vaudenay, Martin Vuagnoux

Instant Ciphertext-Only Cryptanalysis of GSM
Encrypted Communication 600
 Elad Barkan, Eli Biham, Nathan Keller

Making a Faster Cryptanalytic Time-Memory Trade-Off 617
 Philippe Oechslin

Author Index 631