# Table of Contents

## Invited Talks

Some Applications of Polynomials for the Design of Cryptographic Protocols . . . 1
*Eyal Kushilevitz (Technion)*

Secure Multi-party Computation Made Simple . . . 14
*Ueli Maurer (ETH)*

## Forward Security

Forward Secrecy in Password-Only Key Exchange Protocols . . . 29
*Jonathan Katz (University of Maryland), Rafail Ostrovsky (Telcordia Technologies, Inc.), and Moti Yung (Columbia University)*

Weak Forward Security in Mediated RSA . . . 45
*Gene Tsudik (University of California, Irvine)*

## Foundations of Cryptography

On the Power of Claw-Free Permutations . . . 55
*Yevgeniy Dodis (New York University) and Leonid Reyzin (Boston University)*

Equivocable and Extractable Commitment Schemes . . . 74
*Giovanni Di Crescenzo (Telcordia Technologies)*

An Improved Pseudorandom Generator Based on Hardness of Factoring . . . 88
*Nenad Dedić, Leonid Reyzin (Boston University), and Salil Vadhan (Harvard University)*

Intrusion-Resilient Signatures: Generic Constructions, or Defeating Strong Adversary with Minimal Assumptions . . . 102
*Gene Itkis (Boston University)*

## Key Management

Efficient Re-keying Protocols for Multicast Encryption . . . 119
*Giovanni Di Crescenzo (Telcordia Technologies) and Olga Kornievskaia (University of Michigan)*

On a Class of Key Agreement Protocols Which Cannot Be Unconditionally Secure . . . 133
*Frank Niedermeyer and Werner Schindler (BSI)*

A Group Key Distribution Scheme with Decentralised User Join ......... 146
*Hartono Kurnio, Rei Safavi-Naini (University of Wollongong), and Huaxiong Wang (Macquarie University)*

## Cryptanalysis

On a Resynchronization Weakness in a Class of Combiners with Memory ........................................................ 164
*Yuri Borissov (Bulgarian Academy of Sciences), Svetla Nikova, Bart Preneel, and Joos Vandewalle (Katholieke Universiteit Leuven)*

On Probability of Success in Linear and Differential Cryptanalysis ....... 174
*Ali Aydın Selçuk (Purdue University) and Ali Bıçak (University of Maryland Baltimore County)*

Differential Cryptanalysis of a Reduced-Round SEED .................. 186
*Hitoshi Yanami and Takeshi Shimoyama (Fujitsu Laboratories LTD)*

## System Security

Medical Information Privacy Assurance: Cryptographic and System Aspects ..................................... 199
*Giuseppe Ateniese, Reza Curtmola, Breno de Medeiros, and Darren Davis (The Johns Hopkins University)*

A *Format-Independent* Architecture for Run-Time Integrity Checking of Executable Code ................................................... 219
*Luigi Catuogno and Ivan Visconti (Università di Salerno)*

## Signature Schemes

How to Repair ESIGN ................................................. 234
*Louis Granboulan (École Normale Supérieure)*

Forward-Secure Signatures with Fast Key Update ...................... 241
*Anton Kozlov and Leonid Reyzin (Boston University)*

Constructing Elliptic Curves with Prescribed Embedding Degrees ........ 257
*Paulo S.L.M. Barreto (Universidade de São Paulo), Ben Lynn (Stanford University), and Michael Scott (Dublin City University)*

A Signature Scheme with Efficient Protocols ........................... 268
*Jan Camenisch (IBM Research) and Anna Lysyanskaya (Brown University)*

## Zero Knowledge

Efficient Zero-Knowledge Proofs for Some Practical Graph Problems ..... 290
*Yvo Desmedt (Florida State University and University of London) and Yongge Wang (University of North Carolina at Charlotte)*

Reduction Zero-Knowledge ..... 303
*Xiaotie Deng, C.H. Lee (City University of Hong Kong), Yunlei Zhao (City University of Hong Kong and Fudan University), and Hong Zhu (Fudan University)*

A New Notion of Soundness in Bare Public-Key Model ..... 318
*Shirley H.C. Cheung, Xiaotie Deng, C.H. Lee (City University of Hong Kong), and Yunlei Zhao (City University of Hong Kong and Fudan University)*

## Information Theory and Secret Sharing

Robust Information-Theoretic Private Information Retrieval ..... 326
*Amos Beimel and Yoav Stahl (Ben-Gurion University)*

Trading Players for Efficiency in Unconditional Multiparty Computation .. 342
*B. Prabhu, K. Srinathan, and C. Pandu Rangan (Indian Institute of Technology)*

Secret Sharing Schemes on Access Structures
with Intersection Number Equal to One ..... 354
*Jaume Martí-Farré and Carles Padró (Universitat Politècnica de Catalunya)*

**Author Index** ..... 365