

Table of Contents

Invited Talks

Some Applications of Polynomials for the Design of Cryptographic Protocols	1
<i>Eyal Kushilevitz (Technion)</i>	
Secure Multi-party Computation Made Simple	14
<i>Ueli Maurer (ETH)</i>	

Forward Security

Forward Secrecy in Password-Only Key Exchange Protocols	29
<i>Jonathan Katz (University of Maryland), Rafail Ostrovsky (Telcordia Technologies, Inc.), and Moti Yung (Columbia University)</i>	
Weak Forward Security in Mediated RSA	45
<i>Gene Tsudik (University of California, Irvine)</i>	

Foundations of Cryptography

On the Power of Claw-Free Permutations	55
<i>Yevgeniy Dodis (New York University) and Leonid Reyzin (Boston University)</i>	
Equivocable and Extractable Commitment Schemes	74
<i>Giovanni Di Crescenzo (Telcordia Technologies)</i>	
An Improved Pseudorandom Generator Based on Hardness of Factoring . .	88
<i>Nenad Dedić, Leonid Reyzin (Boston University), and Salil Vadhan (Harvard University)</i>	
Intrusion-Resilient Signatures: Generic Constructions, or Defeating Strong Adversary with Minimal Assumptions	102
<i>Gene Itkis (Boston University)</i>	

Key Management

Efficient Re-keying Protocols for Multicast Encryption	119
<i>Giovanni Di Crescenzo (Telcordia Technologies) and Olga Kornievskaia (University of Michigan)</i>	
On a Class of Key Agreement Protocols Which Cannot Be Unconditionally Secure	133
<i>Frank Niedermeyer and Werner Schindler (BSI)</i>	

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

Cryptanalysis

On a Resynchronization Weakness in a Class of Combiners with Memory	164
<i>Yuri Borissov (Bulgarian Academy of Sciences), Svetla Nikova, Bart Preneel, and Joos Vandewalle (Katholieke Universiteit Leuven)</i>	
On Probability of Success in Linear and Differential Cryptanalysis	174
<i>Ali Aydın Selçuk (Purdue University) and Ali Bıçak (University of Maryland Baltimore County)</i>	
Differential Cryptanalysis of a Reduced-Round SEED	186
<i>Hitoshi Yanami and Takeshi Shimoyama (Fujitsu Laboratories LTD)</i>	

System Security

Medical Information Privacy Assurance: Cryptographic and System Aspects	199
<i>Giuseppe Ateniese, Reza Curtmola, Breno de Medeiros, and Darren Davis (The Johns Hopkins University)</i>	
A Format-Independent Architecture for Run-Time Integrity Checking of Executable Code	219
<i>Luigi Catuogno and Ivan Visconti (Università di Salerno)</i>	

Signature Schemes

How to Repair ESIGN	234
<i>Louis Granboulan (École Normale Supérieure)</i>	
Forward-Secure Signatures with Fast Key Update	241
<i>Anton Kozlov and Leonid Reyzin (Boston University)</i>	
Constructing Elliptic Curves with Prescribed Embedding Degrees	257
<i>Paulo S.L.M. Barreto (Universidade de São Paulo), Ben Lynn (Stanford University), and Michael Scott (Dublin City University)</i>	
A Signature Scheme with Efficient Protocols	268
<i>Jan Camenisch (IBM Research) and Anna Lysyanskaya (Brown University)</i>	

Zero Knowledge

Efficient Zero-Knowledge Proofs for Some Practical Graph Problems	290
<i>Yvo Desmedt (Florida State University and University of London)</i> <i>and Yongge Wang (University of North Carolina at Charlotte)</i>	
Reduction Zero-Knowledge	303
<i>Xiaotie Deng, C.H. Lee (City University of Hong Kong),</i> <i>Yunlei Zhao (City University of Hong Kong and Fudan University),</i> <i>and Hong Zhu (Fudan University)</i>	
A New Notion of Soundness in Bare Public-Key Model	318
<i>Shirley H.C. Cheung, Xiaotie Deng, C.H. Lee (City University of Hong Kong),</i> <i>and Yunlei Zhao (City University of Hong Kong and Fudan University)</i>	

Information Theory and Secret Sharing

Robust Information-Theoretic Private Information Retrieval	326
<i>Amos Beimel and Yoav Stahl (Ben-Gurion University)</i>	
Trading Players for Efficiency in Unconditional Multiparty Computation . .	342
<i>B. Prabh, K. Srinathan, and C. Pandu Rangan (Indian Institute of Technology)</i>	
Secret Sharing Schemes on Access Structures with Intersection Number Equal to One	354
<i>Jaume Martí-Farré and Carles Padró (Universitat Politècnica de Catalunya)</i>	
Author Index	365

Security in Communication Networks

Third International Conference, SCN 2002, Amalfi, Italy,

September 11-13, 2002, Revised Papers

Cimato, S.; Galdi, C.; Persiano, G. (Eds.)

2003, IX, 263 p., Softcover

ISBN: 978-3-540-00420-2