

Table of Contents

Factoring and Discrete Logarithm

Factorization of a 512-Bit RSA Modulus	1
<i>Stefania Cavallar (CWI, The Netherlands), Bruce Dodson (Lehigh University, USA), Arjen K. Lenstra (Citibank, USA), Walter Lioen (CWI, The Netherlands), Peter L. Montgomery (Microsoft Research, USA and CWI, The Netherlands), Brian Murphy (Computer Sciences Laboratory, Australia), Herman te Riele (CWI, The Netherlands), Karen Aardal (Utrecht University, The Netherlands), Jeff Gilchrist (Entrust Technologies Ltd., Canada), Gérard Guillerm (École Polytechnique, France), Paul Leyland (Microsoft Research Ltd., UK), Joël Marchand (École Polytechnique/CNRS, France), François Morain (École Polytechnique, France), Alec Muffett (Sun Microsystems Professional Services, UK), Chris and Craig Putnam (USA), Paul Zimmermann (Inria Lorraine and Loria, France)</i>	
An Algorithm for Solving the Discrete Log Problem on Hyperelliptic Curves	19
<i>Pierrick Gaudry (École Polytechnique, France)</i>	
Analysis and Optimization of the TWINKLE Factoring Device	35
<i>Arjen K. Lenstra (Citibank, USA), Adi Shamir (The Weizmann Institute, Israel)</i>	

Cryptanalysis I: Digital Signatures

Noisy Polynomial Interpolation and Noisy Chinese Remaindering	53
<i>Daniel Bleichenbacher (Bell Laboratories, USA), Phong Q. Nguyen (École Normale Supérieure, France)</i>	
A Chosen Messages Attack on the ISO/IEC 9796-1 Signature Scheme	70
<i>François Grieu (Innovatron, France)</i>	
Cryptanalysis of Countermeasures Proposed for Repairing ISO 9796-1	81
<i>Marc Girault, Jean-François Misarsky (France Télécom - CNET, France)</i>	
Security Analysis of the Gennaro-Halevi-Rabin Signature Scheme	91
<i>Jean-Sébastien Coron (École Normale Supérieure, France), David Naccache (Gemplus Card International, France)</i>	

Invited Talk

On the Security of 3GPP Networks	102
<i>Michael Walker (Vodafone and Royal Holloway College, University of London, UK)</i>	

Private Information Retrieval

One-Way Trapdoor Permutations Are Sufficient for Non-trivial Single-Server Private Information Retrieval	104
<i>Eyal Kushilevitz (IBM T.J. Watson Research Center, USA), Rafail Ostrovsky (Telcordia Technologies Inc., USA)</i>	

Single Database Private Information Retrieval Implies Oblivious Transfer	122
<i>Giovanni Di Crescenzo (Telcordia Technologies, Inc., USA), Tal Malkin (Massachusetts Institute of Technology and AT&T Labs Research), Rafail Ostrovsky (Telcordia Technologies, Inc., USA)</i>	

Key Management Protocols

Authenticated Key Exchange Secure against Dictionary Attacks	139
<i>Mihir Bellare (University of California at San Diego, USA), David Pointcheval (École Normale Supérieure, France), Phillip Rogaway (University of California at Davis, USA)</i>	

Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman	156
<i>Victor Boyko (Massachusetts Institute of Technology, USA), Philip MacKenzie (Bell Laboratories, USA), Sarvar Patel (Bell Laboratories, USA)</i>	

Fair Encryption of RSA Keys	172
<i>Guillaume Poupard, Jacques Stern (École Normale Supérieure, France)</i>	

Threshold Cryptography and Digital Signatures

Computing Inverses over a Shared Secret Modulus	190
<i>Dario Catalano (Università di Catania, Italy), Rosario Gennaro (IBM T.J. Watson Research Center, USA), Shai Halevi (IBM T.J. Watson Research Center, USA)</i>	

Practical Threshold Signatures	207
<i>Victor Shoup (IBM Zürich Research Laboratory, Switzerland)</i>	

Adaptively Secure Threshold Cryptography: Introducing Concurrency, Removing Erasures	221
<i>Stanisław Jarecki, Anna Lysyanskaya (Massachusetts Institute of Technology, USA)</i>	

Confirmer Signature Schemes Secure against Adaptive Adversaries	243
<i>Jan Camenisch (IBM Zürich Research Laboratory, Switzerland),</i>	
<i>Markus Michels (Entrust Technologies, Switzerland)</i>	

Public-Key Encryption

Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements	259
<i>Mihir Bellare (University of California at San Diego, USA),</i>	
<i>Alexandra Boldyreva (University of California at San Diego, USA),</i>	
<i>Silvio Micali (Massachusetts Institute of Technology, USA)</i>	
Using Hash Functions as a Hedge against Chosen Ciphertext Attack	275
<i>Victor Shoup (IBM Zürich Research Laboratory, Switzerland)</i>	

Quantum Cryptography

Security Aspects of Practical Quantum Cryptography	289
<i>Gilles Brassard (Université de Montréal, Canada), Norbert Lütkenhaus</i>	
<i>(Helsinki Institute of Physics, Finland), Tal Mor (University of</i>	
<i>California at Los Angeles, USA and College of Judea and Samaria,</i>	
<i>Israel), Barry C. Sanders (Macquarie University, Australia)</i>	
Perfectly Concealing Quantum Bit Commitment from any Quantum One-Way Permutation	300
<i>Paul Dumais (Université de Montréal, Canada),</i>	
<i>Dominic Mayers (NEC Research Institute, USA),</i>	
<i>Louis Salvail (BRICS, University of Århus, Denmark)</i>	

Multi-party Computation and Information Theory

General Secure Multi-party Computation from any Linear Secret-Sharing Scheme	316
<i>Ronald Cramer (BRICS, Aarhus University, Denmark),</i>	
<i>Ivan Damgård (BRICS, Aarhus University, Denmark),</i>	
<i>Ueli Maurer (ETH Zürich, Switzerland)</i>	
Minimal-Latency Secure Function Evaluation	335
<i>Donald Beaver (CertCo Inc., USA)</i>	
Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free	351
<i>Ueli Maurer, Stefan Wolf (ETH Zürich, Switzerland)</i>	

Cryptanalysis II: Public-Key Encryption

New Attacks on PKCS#1 v1.5 Encryption	369
<i>Jean-Sébastien Coron (École Normale Supérieure and Gemplus Card International, France), Marc Joye (Gemplus Card International, France), David Naccache (Gemplus Card International, France), Pascal Paillier (Gemplus Card International, France)</i>	
A NICE Cryptanalysis	382
<i>Éliane Jaulmes, Antoine Joux (SCSSI, France)</i>	
Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations	392
<i>Nicolas Courtois (Toulon University and Bull CP8, France), Alexander Klimov (Moscow State University, Russia), Jacques Patarin (Bull CP8, France), Adi Shamir (The Weizmann Institute of Science, Israel)</i>	
Cryptanalysis of Patarin's 2-Round Public Key System with S Boxes (2R)	408
<i>Eli Biham (Technion, Israel)</i>	

Invited Talk

Colossus and the German Lorenz Cipher – Code Breaking in WW II	417
<i>Anthony E Sale (Bletchley Park Trust)</i>	

Zero-Knowledge

Efficient Concurrent Zero-Knowledge in the Auxiliary String Model	418
<i>Ivan Damgård (BRICS, Aarhus University, Denmark)</i>	
Efficient Proofs that a Committed Number Lies in an Interval	431
<i>Fabrice Boudot (France Télécom - CNET, France)</i>	

Symmetric Cryptography

A Composition Theorem for Universal One-Way Hash Functions	445
<i>Victor Shoup (IBM Zürich Research Laboratory, Switzerland)</i>	
Exposure-Resilient Functions and All-Or-Nothing Transforms	453
<i>Ran Canetti (IBM T.J. Watson Research Center, USA), Yevgeniy Dodis (Massachusetts Institute of Technology, USA), Shai Halevi (IBM T.J. Watson Research Center, USA), Eyal Kushilevitz (IBM T.J. Watson Research Center, USA and Technion, Israel), Amit Sahai (Massachusetts Institute of Technology, USA)</i>	
The Sum of PRPs Is a Secure PRF	470
<i>Stefan Lucks (Universität Mannheim, Germany)</i>	

Boolean Functions and Hardware

Construction of Nonlinear Boolean Functions with Important Cryptographic Properties	485
<i>Palash Sarkar, Subhamoy Maitra (Indian Statistical Institute, India)</i>	
Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions	507
<i>Anne Canteaut (INRIA, France), Claude Carlet (Université de Caen, France), Pascale Charpin (INRIA, France), Caroline Fontaine (Université des Sciences et Technologies de Lille, France)</i>	
Cox-Rower Architecture for Fast Parallel Montgomery Multiplication	523
<i>Shinichi Kawamura, Masanobu Koike, Fumihiko Sano, Atsushi Shimbo (Toshiba Corporation, Japan)</i>	

Voting Schemes

Efficient Receipt-Free Voting Based on Homomorphic Encryption	539
<i>Martin Hirt (ETH Zürich, Switzerland), Kazuo Sako (NEC Corporation, Japan)</i>	
How to Break a Practical MIX and Design a New One	557
<i>Yvo Desmedt (Florida State University, USA and Royal Holloway, University of London, UK), Kaoru Kurosawa (Tokyo Institute of Technology, Japan)</i>	

Cryptanalysis III: Stream Ciphers and Block Ciphers

Improved Fast Correlation Attacks Using Parity-Check Equations of Weight 4 and 5	573
<i>Anne Canteaut (INRIA, France), Michaël Trabbia (INRIA and École Polytechnique, France)</i>	
Advanced Slide Attacks	589
<i>Alex Biryukov (Technion, Israel), David Wagner (University of California at Berkeley, USA)</i>	

Author Index	607
------------------------	-----

Advances in Cryptology - EUROCRYPT 2000
International Conference on the Theory and Application
of Cryptographic Techniques Bruges, Belgium, May
14-18, 2000 Proceedings
Preneel, B. (Ed.)
2000, XIII, 612 p., Softcover
ISBN: 978-3-540-67517-4