# Eurocrypt 2000

*Bruges (Brugge), Belgium, May 14-18, 2000*

## PROGRAM

### Sunday May 14, 2000

| | |
|---|---|
| *17:00-20:00* | **Registration** |
| *19:00-20:30* | **Reception** *(Provinciaal Hof)* |

### Monday May 15, 2000

| | |
|---|---|
| *08:00* | **Registration** |
| *08:50-9:00* | **Welcome** |

**Session 1: Factoring and Discrete Logarithm** — *Chair: Bart Preneel*

| | |
|---|---|
| *09:00-09:25* | **Factorization of a 512-bit RSA Modulus**<br>*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 (The Australian National University, 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, UK), Chris and Craig Putnam (USA), Paul Zimmermann (Inria Lorraine and Loria, France)* |
| *09:25-09:50* | **An Algorithm for Solving the Discrete Log Problem on Hyperelliptic Curves**<br>*Pierrick Gaudry (École Polytechnique, France)* |
| *09:50-10:15* | **Analysis and Optimization of the TWINKLE Factoring Device**<br>*Arjen K. Lenstra (Citibank, USA), Adi Shamir (The Weizmann Institute, Israel)* |
| *10:15-10:45* | **Coffee Break** |

**Session 2: Cryptanalysis I: Digital Signatures** — *Chair: Hans Dobbertin*

| | |
|---|---|
| *10:45-11:10* | **Noisy Polynomial Interpolation and Noisy Chinese Remaindering**<br>*Daniel Bleichenbacher (Bell Laboratories, USA), Phong Q. Nguyen (École Normale Supérieure, France)* |
| *11:10-11:35* | **A Chosen Message Attack on the ISO/IEC 9796-1 Signature Scheme**<br>*François Grieu (Innovatron, France)* |
| *11:35-12:00* | **Cryptanalysis of Countermeasures Proposed for Repairing ISO 9796-1**<br>*Marc Girault, Jean-François Misarsky (France Télécom - CNET, France)* |
| *12:00-12:25* | **Security Analysis of the Gennaro-Halevi-Rabin Signature Scheme**<br>*Jean-Sébastien Coron (École Normale Supérieure, France), David Naccache (Gemplus Card International, France)* |
| *12:25-14:00* | **Lunch** |

**Session 3: Invited Talk** — *Chair: Kaisa Nyberg*

| | |
|---|---|
| *14:00-14:50* | **On the Security of 3GPP Networks** (invited)<br>*Mike Walker (Vodafone, UK)* |

**Session 4: Private Information Retrieval** — *Chair: Christian Cachin*



| | |
|---|---|
| *14:50-15:15* | **One-way Trapdoor Permutations Are Sufficient for Non-Trivial Single-Server Private Information Retrieval**<br>*Eyal Kushilevitz (IBM T.J. Watson Research Center, USA), Rafail Ostrovsky (Telcordia Technologies Inc., USA)* |
| *15:15-15:40* | **Single Database Private Information Retrieval Implies Oblivious Transfer**<br>*Giovanni Di Crescenzo (Telcordia Technologies Inc., USA), Tal Malkin (AT&T Labs Research, (work done at Massachusetts Institute of Technology) USA), Rafail Ostrovsky (Telcordia Technologies Inc., USA)* |
| *15:40-16:10* | **Coffee Break** |

**Session 5: Key Management Protocols** — *Chair: Paul van Oorschot*

| | |
|---|---|
| *16:10-16:35* | **Authenticated Key Exchange Secure Against Dictionary Attacks**<br>*Mihir Bellare (University of California at San Diego, USA), David Pointcheval (École Normale Supérieure, France), Phillip Rogaway (University of California at Davis, USA)* |
| *16:35-17:00* | **Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman**<br>*Victor Boyko (Massachusetts Institute of Technology,USA), Philip MacKenzie (Bell Laboratories, USA), Sarvar Patel (Bell Laboratories, Lucent Technologies, USA)* |
| *17:00-17:25* | **Fair Encryption of RSA Keys**<br>*Guillaume Poupard, Jacques Stern (École Normale Supérieure, France)* |

### Tuesday May 16, 2000

**Session 6: Threshold Cryptography and Digital Signatures** — *Chair: Torben Pedersen*

| | |
|---|---|
| ***08:35-09:00***<br>*early start!* | **Computing Inverses Over a Shared Secret Modulus**<br>*Dario Catalano (Universitá di Catania, Italy), Rosario Gennaro (IBM T.J.Watson Research Center, USA), Shai Halevi (IBM T.J.Watson Research Center, USA)* |
| *09:00-09:25* | **Practical Threshold Signatures**<br>*Victor Shoup (IBM Zürich Research Laboratory, Switzerland)* |
| *09:25-09:50* | **Adaptively Secure Threshold Cryptography: Introducing Concurrency, Removing Erasures**<br>*Stanislaw Jarecki, Anna Lysyanskaya (Massachusetts Institute of Technology, USA)* |
| *09:50-10:15* | **Confirmer Signature Schemes Secure against Adaptive Adversaries**<br>*Jan Camenisch (IBM Zürich Research Laboratory,Switzerland), Markus Michels (Entrust Technologies, Switzerland)* |
| *10:15-10:45* | **Coffee Break** |

**Session 7: Public-Key Encryption** — *Chair: David Pointcheval*

| | |
|---|---|
| *10:45-11:10* | **Public-key Encryption in a Multi-User Setting: Security Proofs and Improvements**<br>*Mihir Bellare (University of California at San Diego, USA), Alexandra Boldyreva (University of California at San Diego, USA), Silvio Micali (Massachusetts Institute of Technology, USA)* |
| *11:10-11:35* | **Using Hash Functions as a Hedge Against Chosen Ciphertext Attack**<br>*Victor Shoup (IBM Zürich Research Laboratory, Switzerland)* |

**Session 8: Quantum Cryptography** — *Chair: Dan Boneh*

| | |
|---|---|
| *11:35-12:00* | **Security Aspects of Practical Quantum Cryptography**<br>*Gilles Brassard (Université de Montréal, Canada), Norbert Lütkenhaus (Helsinki Institute of Physics, Finland), Tal Mor (University of California at Los Angeles, CA, USA and College of Judea and Samaria, Israel), Barry C. Sanders (Macquarie University, Australia)* |

| | |
|---|---|
| *12:00-12:25* | **Perfectly Concealing Quantum Bit Commitment from Any One-Way Permutation**<br>*Paul Dumais (Université de Montréal, Canada), Dominic Mayers (NEC Research Institute, Princeton, USA), Louis Salvail (BRICS, Aarhus University, Denmark)* |
| *12:25-14:00* | **Lunch** |

## *Rump Session* — *Chair: Andy Clark*

| | |
|---|---|
| *19:00-20:00* | **Poster session** - *Program will be determined during the conference* |
| *20:00-20:45* | **Rump session I** |
| *20:45-21:30* | **Poster session** |
| *21:30-22:15* | **Rump session II** |

# *Wednesday May 17, 2000*

## *Session 9: Multi-Party Computation and Information Theory* — *Chair: Moti Yung*

| | |
|---|---|
| *09:00-09:25* | **General Secure Multi-Party Computation from any Linear Secret-Sharing Scheme**<br>*Ronald Cramer (BRICS, Aarhus University, Denmark (work done while at ETH Zürich, Switzerland)), Ivan Damgård (BRICS, Aarhus University, Denmark), Ueli Maurer (ETH Zürich, Switzerland)* |
| *09:25-09:50* | **Minimal-Latency Secure Function Evaluation**<br>*Donald Beaver (CertCo, USA)* |
| *09:50-10:15* | **Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free**<br>*Ueli Maurer, Stefan Wolf (ETH Zürich, Switzerland)* |
| *10:15-10:45* | **Coffee Break** |

## *Session 10: Cryptanalysis II: Public-Key Encryption* — *Chair: Jean-Jacques Quisquater*

| | |
|---|---|
| *10:45-11:10* | **New Attacks on PKCS#1 v1.5 Encryption**<br>*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)* |
| *11:10-11:35* | **A NICE Cryptanalysis**<br>*Éliane Jaulmes, Antoine Joux (SCSSI, France)* |
| *11:35-12:00* | **Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations**<br>*Nicolas Courtois (Toulon University, France), Alexander Klimov (Moscow State University, Russia), Jacques Patarin (Bull CP8, France), Adi Shamir (The Weizmann Institute of Science, Israel)* |
| *12:00-12:25* | **Cryptanalysis of Patarin's 2-Round Public Key System with S Boxes (2R)**<br>*Eli Biham (Technion - Israel Institute of Technology, Israel)* |
| *12:25-14:00* | **Lunch** |

## *Session 11: Invited Talk* — *Chair: Whitfield Diffie*

| | |
|---|---|
| *14:00-14:50* | **Colossus and the German Lorenz Cipher** (invited)<br>*A.E. Sale (Bletchley Park Trust)* |

## *Session 12: Zero Knowledge* — *Chair: Ronald Cramer*

| | |
|---|---|
| *14:50-15:15* | **Efficient Concurrent Zero-Knowledge in the Auxiliary String Model**<br>*Ivan Damgård (BRICS, Aarhus University, Denmark)* |
| *15:15-15:40* | **Efficient Proofs that a Committed Number Lies in an Interval**<br>*Fabrice Boudot (France Télécom - CNET, France)* |
| *15:40-16:10* | **Coffee Break** |



## *Session 13:Symmetric Cryptography* — *Chair: Mitsuru Matsui*

| | |
|---|---|
| *16:10-16:35* | **A Composition Theorem for Universal One-Way Hash Functions**<br>*Victor Shoup (IBM Zürich Research Laboratory, Switzerland)* |
| *16:35-17:00* | **Exposure Resilient Functions and All-or-Nothing Transforms**<br>*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), Amit Sahai (Massachusetts Institute of Technology, USA)* |
| *17:00-17:25* | **The Sum of PRPs is a Secure PRF**<br>*Stefan Lucks (Universität Mannheim, Germany)* |
| *17:30-18:15* | **IACR Business Meeting** |
| *19:30-23:00* | **Conference Dinner** |

# *Thursday May 18, 2000*

## *Session 14: Boolean Functions and Hardware* — *Chair: Thomas Johansson*

| | |
|---|---|
| *09:00-09:25* | **Construction of Nonlinear Boolean Functions with Important Cryptographic Properties**<br>*Palash Sarkar, Subhamoy Maitra (Indian Statistical Institute, India)* |
| *09:25-09:50* | **Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions**<br>*Anne Canteaut (INRIA, France), Claude Carlet (Université de Caen, France), Pascale Charpin (INRIA, France), Caroline Fontaine (Université des Sciences et Technologie de Lille, France)* |
| *09:50-10:15* | **Cox-Rower Architecture for Fast Parallel Montgomery Multiplication**<br>*Shinichi Kawamura, Masanobu Koike, Fumihiko Sano, Atsushi Shimbo (Toshiba Corporation, Japan)* |
| *10:15-10:45* | **Coffee Break** |

## *Session 15: Voting Schemes* — *Chair: Markus Jakobsson*

| | |
|---|---|
| *10:45-11:10* | **Efficient Receipt-Free Voting Based on Homomorphic Encryption**<br>*Martin Hirt (ETH Zürich, Switzerland), Kazue Sako (NEC Corporation, Japan)* |
| *11:10-11:35* | **How to Break a Practical MIX and Design a New One**<br>*Yvo Desmedt (Florida State University, USA and Royal Holloway, UK), Kaoru Kurosawa (Tokyo Institute of Technology, Japan)* |

## *Session 16: Cryptanalysis III: Stream Ciphers and Block Ciphers* — *Chair: Lars Knudsen*

| | |
|---|---|
| *11:35-12:00* | **Improved Fast Correlation Attacks Using Parity-Check Equations of Weight 4 and 5**<br>*Anne Canteaut (INRIA, France), Michaël Trabbia (École Polytechnique, France)* |
| *12:00-12:25* | **Advanced Slide Attacks**<br>*Alex Biryukov (Technion - Israel Institute of Technology, Israel), David Wagner (University of California at Berkeley, USA)* |
| *12:25-14:00* | **Lunch** |

***Eurocrypt 2000 is organized by the members of the COSIC research group.***