Preface

EUROCRYPT 2000, the nineteenth annual Eurocrypt Conference, was sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the Katholieke Universiteit Leuven in Belgium (research group for Computer Security and Industrial Cryptography, COSIC).

The first conference with the name 'Eurocrypt' took place in 1983, but the 1982 Workshop at Burg Feuerstein was the first open meeting in Europe on cryptology; it has been included in Lecture Notes in Computer Science 1440, which contains an electronic proceedings and index of the Crypto and Eurocrypt conferences 1981–1997.

The program committee considered 150 papers and selected 39 for presentation. One paper was withdrawn by the authors. The program also included invited talks by Michael Walker ("On the Security of 3GPP Networks") and Tony Sale ("Colossus and the German Lorenz Cipher – Code Breaking in WW II"). In addition, Andy Clark kindly agreed to chair the traditional rump session for informal presentations of recent results.

The selection of the program was a challenging task, as many high quality submissions were received. Each submission was reviewed by at least three reviewers and most reports had four or more reviews (papers with program committee members as a co-author had at least six reviews). The program committee worked very hard to evaluate the papers with respect to quality, originality, and relevance to cryptology. In most cases they were able to provide extensive comments to the authors (about half a Megabyte of comments for authors has been written). Subsequently, the authors of accepted papers have made a substantial effort to take into account the comments in the version submitted to these proceedings. In a limited number of cases, these revisions have been checked by members of the program committee.

First and foremost I would like to thank the members of the program committee for the many hours spent on reviewing and discussing the papers, and for helping me with the difficult decisions.

I gratefully acknowledge the help of a large number of colleagues who reviewed submissions in their area of expertise: Masayuki Abe, N. Asokan, Olivier Baudron, Josh Benaloh, Eli Biham, Simon Blake-Wilson, Johan Borst, Emmanuel Bresson, Jan Camenisch, Ivan Damgård, Anand Desai, Yvo Desmedt, Glenn Durfee, Serge Fehr, Matthias Fitzi, Pierre-Alain Fouque, Matt Franklin, Steven Galbraith, Juan A. Garay, Louis Granboulan, Stuart Haber, Shai Halevi, Martin Hirt, Fredrik Jönsson, Mike Jacobson, Jens G. Jensen, Ari Juels, Jonathan Katz, Robert Lambert, Julio Lopez Hernandez, Phil MacKenzie, Julien Marcil, Willi Meier, Preda Mihailescu, Serge Mister, Fabian Monrose, Sean Murphy, Siaw-Lynn Ng, Phong Nguyen, Valtteri Niemi, Tatsuaki Okamoto, Thomas Pornin, Guillaume Poupard, Bartek Przydatek, Omer Reingold, Vincent Rijmen, Louis Salvail, Tomas Sander, Berry Schoenmakers, Dan Simon, Ben Smeets,

Michael Steiner, Jacques Stern, Martin Strauss, Katsuyuki Takashima, Edlyn Teske, Barry Trager, Ramarathnam Venkatesan, Frederik Vercauteren, Susanne Wetzel, Mike Wiener, Peter Wild, Adam Young. I apologise for any inadvertent omissions.

By now, electronic submissions have become a tradition for Eurocrypt. I would like to thank Joe Kilian, who did an excellent job in running the electronic submission server of ACM's SIGACT group. Only five contributions were submitted in paper form; for three of these, I obtained an electronic copy from the authors. The remaining two papers were scanned in to make the process uniform to reviewers. As a first for IACR sponsored conferences, we developed a web interface for entering reviews and discussing papers. Special thanks go to Joris Claessens and Wim Moreau who spent several weeks developing my rough specifications into a flawless program with a smooth user interface. This work made the job of the program committee much easier, as we could focus on the content of the discussion rather than on its organisation. This software will be made available to all IACR sponsored conferences.

My ability to run the program committee was increased substantially by the effort and skills provided by the members of COSIC: Vincent Rijmen put together the LaTeX version of the proceedings, Joris Claessens helped with processing the submissions, Johan Borst converted a paper to LaTeX, Péla Noë assisted with organising the program committee meeting, and (last but not least) Wim Moreau helped with the electronic processing of the submissions and final versions, and with the copyright forms.

I would like to thank Joos Vandewalle, general chair, the members of the organising committee (Joris Claessens, Danny De Cock, Erik De Win, Marijke De Soete, Keith Martin, Wim Moreau, Péla Noë, Jean-Jacques Quisquater, Vincent Rijmen, Bart Van Rompay, Karel Wouters), and the other members of COSIC for their support. I also thank Elvira Wouters, who took care of the accounting, and Anne De Smet (Momentum), who was responsible for the hotel bookings and the social program. For the first time, the registrations of Eurocrypt were handled by the IACR General Secretariat in Santa Barbara (UCSB); I would like to thank Micky Swick and Sally Vito for the successful collaboration. The organising committee gratefully acknowledges the financial contributions of our sponsors: Isabel, Ubizen, Europay International, Cryptomathic Belgium, PriceWaterhouseCoopers, Utimaco, and the Katholieke Universiteit Leuven.

Finally, I wish to thank all the authors who submitted papers, making this conference possible, and the authors of accepted papers for their cooperation. Special thanks go to Alfred Hofmann and his colleagues at Springer-Verlag for the timely production of this volume.

March 2000

Bart Preneel
Program Chair
Eurocrypt 2000

EUROCRYPT 2000

May 14–18, 2000, Bruges, Belgium

Sponsored by the

International Association for Cryptologic Research

General Chair

Joos Vandewalle, Katholieke Universiteit Leuven, Belgium

Program Chair

Bart Preneel, Katholieke Universiteit Leuven, Belgium

Program Committee

Simon Blackburn ..... Royal Holloway Univ. of London, UK
Dan Boneh ..... Stanford Univ., USA
Christian Cachin ..... IBM Research, Switzerland
Don Coppersmith ..... IBM Research, USA
Ronald Cramer ..... ETH Zurich, Switzerland
Hans Dobbertin ..... BSI, Germany
Markus Jakobsson ..... Bell Laboratories, USA
Thomas Johansson ..... Lund Univ., Sweden
Joe Kilian ..... NEC Research Institute, USA
Lars Knudsen ..... Univ. of Bergen, Norway
Mitsuru Matsui ..... Mitsubishi, Japan
Alfred Menezes ..... Univ. of Waterloo, Canada
Moni Naor ..... Weizmann Institute of Science, Israel
Kaisa Nyberg ..... Nokia Research Center, Finland
Paul van Oorschot ..... Entrust Technologies, Canada
Torben Pedersen ..... Cryptomathic, Denmark
David Pointcheval ..... ENS, France
Moti Yung ..... Certco, USA

Table of Contents

Factoring and Discrete Logarithm

Factorization of a 512–bit RSA Modulus 1
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)

An Algorithm for Solving the Discrete Log Problem on Hyperelliptic Curves 19
Pierrick Gaudry (École Polytechnique, France)

Analysis and Optimization of the TWINKLE Factoring Device 35
Arjen K. Lenstra (Citibank, USA), Adi Shamir (The Weizmann Institute, Israel)

Cryptanalysis I: Digital Signatures

Noisy Polynomial Interpolation and Noisy Chinese Remaindering 53
Daniel Bleichenbacher (Bell Laboratories, USA), Phong Q. Nguyen (École Normale Supérieure, France)

A Chosen Messages Attack on the ISO/IEC 9796–1 Signature Scheme 70
François Grieu (Innovatron, France)

Cryptanalysis of Countermeasures Proposed for Repairing ISO 9796-1 81
Marc Girault, Jean-François Misarsky (France Télécom - CNET, France)

Security Analysis of the Gennaro-Halevi-Rabin Signature Scheme 91
Jean-Sébastien Coron (École Normale Supérieure, France), David Naccache (Gemplus Card International, France)

Invited Talk

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

Private Information Retrieval

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

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

Key Management Protocols

Authenticated Key Exchange Secure Against Dictionary Attacks 140
Mihir Bellare (University of California at San Diego, USA), David Pointcheval (École Normale Supérieure, France), Phillip Rogaway (University of California at Davis, USA)

Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman 157
Victor Boyko (Massachusetts Institute of Technology, USA), Philip MacKenzie (Bell Laboratories, USA), Sarvar Patel (Bell Laboratories, USA)

Fair Encryption of RSA Keys 173
Guillaume Poupard, Jacques Stern (École Normale Supérieure, France)

Threshold Cryptography and Digital Signatures

Computing Inverses over a Shared Secret Modulus 191
Dario Catalano (Università di Catania, Italy), Rosario Gennaro (IBM T.J.Watson Research Center, USA), Shai Halevi (IBM T.J.Watson Research Center, USA)

Practical Threshold Signatures 209
Victor Shoup (IBM Zurich Research Laboratory, Switzerland)

Adaptively Secure Threshold Cryptography: Introducing Concurrency, Removing Erasures 223
Stanisław Jarecki, Anna Lysyanskaya (Massachusetts Institute of Technology, USA)

Confirmer Signature Schemes Secure against Adaptive Adversaries 246
Jan Camenisch (IBM Zurich Research Laboratory, Switzerland), Markus Michels (Entrust Technologies, Switzerland)

Public-Key Encryption

Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements 262
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)

Using Hash Functions as a Hedge against Chosen Ciphertext Attack 279
Victor Shoup (IBM Zurich Research Laboratory, Switzerland)

Quantum Cryptography

Security Aspects of Practical Quantum Cryptography 294
Gilles Brassard (Université de Montréal, Canada), Norbert Lütkenhaus (Helsinki Institute of Physics, Finland), Tal Mor (University of California at Los Angeles, USA and College of Judea and Samaria, Israel), Barry C. Sanders (Macquarie University, Australia)

Perfectly Concealing Quantum Bit Commitment from any Quantum One-Way Permutation 305
Paul Dumais (Université de Montréal, Canada), Dominic Mayers (NEC Research Institute, USA), Louis Salvail (BRICS, University of Århus, Denmark)

Multi-Party Computation and Information Theory

General Secure Multi-Party Computation from any Linear Secret-Sharing Scheme 321
Ronald Cramer (BRICS, Aarhus University, Denmark), Ivan Damgård (BRICS, Aarhus University, Denmark), Ueli Maurer (ETH Zurich, Switzerland)

Minimal-Latency Secure Function Evaluation 340
Donald Beaver (CertCo Inc., USA)

Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free 356
Ueli Maurer, Stefan Wolf (ETH Zurich, Switzerland)

Cryptanalysis II: Public-Key Encryption

New Attacks on PKCS#1 v1.5 Encryption 374
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)

A NICE Cryptanalysis 388
Éliane Jaulmes, Antoine Joux (SCSSI, France)

Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations 398
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)

Cryptanalysis of Patarin's 2-Round Public Key System with S Boxes (2R) 414
Eli Biham (Technion, Israel)

Invited Talk

Colossus and the German Lorenz Cipher – Code Breaking in WW II 423
Anthony E Sale (Bletchley Park Trust)

Zero-Knowledge

Efficient Concurrent Zero-Knowledge in the Auxiliary String Model 424
Ivan Damgård (BRICS, Aarhus University, Denmark)

Efficient Proofs that a Committed Number Lies in an Interval 437
Fabrice Boudot (France Télécom - CNET, France)

Symmetric Cryptography

A Composition Theorem for Universal One-Way Hash Functions 451
Victor Shoup (IBM Zurich Research Laboratory, Switzerland)

Exposure-Resilient Functions and All-Or-Nothing Transforms 459
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)

The Sum of PRPs is a Secure PRF 476
Stefan Lucks (Universität Mannheim, Germany)

Boolean Functions and Hardware

Construction of Nonlinear Boolean Functions with Important Cryptographic Properties 491
Palash Sarkar, Subhamoy Maitra (Indian Statistical Institute, India)

Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions 513
Anne Canteaut (INRIA, France), Claude Carlet (Université de Caen, France), Pascale Charpin (NRIA, France), Caroline Fontaine (Université des Sciences et Technologies de Lille, France)

Cox-Rower Architecture for Fast Parallel Montgomery Multiplication 529
Shinichi Kawamura, Masanobu Koike, Fumihiko Sano, Atsushi Shimbo (Toshiba Corporation, Japan)

Voting Schemes

Efficient Receipt-Free Voting Based on Homomorphic Encryption 545
Martin Hirt (ETH Zurich, Switzerland), Kazue Sako (NEC Corporation, Japan)

How to Break a Practical MIX and Design a New One 563
Yvo Desmedt (Florida State University, USA and Royal Holloway, University of London, UK), Kaoru Kurosawa (Tokyo Institute of Technology, Japan)

Cryptanalysis III: Stream Ciphers and Block Ciphers

Improved Fast Correlation Attacks Using Parity-Check Equations of Weight 4 and 5 579
Anne Canteaut (INRIA, France), Michaël Trabbia (INRIA and École Polytechnique, France)

Advanced Slide Attacks 595
Alex Biryukov (Technion, Israel), David Wagner (University of California at Berkeley, USA)

Author Index 613