EUROCRYPT 2000 ONLINE GUIDE

Preface

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 One paper was withdrawn by the authors.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 (IACR)

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

Factorization of a 512–bit RSA Modulus

Stefania Cavallar[3], Bruce Dodson[8], Arjen K. Lenstra[1], Walter Lioen[3], Peter L. Montgomery[10], Brian Murphy[2], Herman te Riele[3], Karen Aardal[13], Jeff Gilchrist[4], Gérard Guillerm[11], Paul Leyland[9], Joël Marchand[5], François Morain[6], Alec Muffett[12], Chris and Craig Putnam[14], and Paul Zimmermann[7]

[1] Citibank, 1 North Gate Road, Mendham, NJ 07945–3104, USA
arjen.lenstra@citicorp.com
[2] Computer Sciences Laboratory, ANU, Canberra ACT 0200, Australia
murphy@cslab.anu.edu.au
[3] CWI, P.O. Box 94079, 1090 GB Amsterdam, The Netherlands
{cavallar,walter,herman}@cwi.nl
[4] Entrust Technologies Ltd., 750 Heron Road, Suite E08, Ottawa, ON,
K1V 1A7, Canada
Jeff.Gilchrist@entrust.com
[5] Laboratoire Gage, École Polytechnique/CNRS, Palaiseau, France
Joel.Marchand@medicis.polytechnique.fr
[6] Laboratoire d'Informatique, École Polytechnique, Palaiseau, France
morain@lix.polytechnique.fr
[7] Inria Lorraine and Loria, Nancy, France
Paul.Zimmermann@loria.fr
[8] Lehigh University, Bethlehem, PA, USA
bad0@Lehigh.edu
[9] Microsoft Research Ltd, Cambridge, UK
pleyland@microsoft.com
[10] 780 Las Colindas Road, San Rafael, CA 94903–2346 USA
Microsoft Research and CWI
pmontgom@cwi.nl
[11] SITX (Centre of IT resources), École Polytechnique, Palaiseau, France
Gerard.Guillerm@polytechnique.fr
[12] Sun Microsystems, Riverside Way, Watchmoor Park, Camberley, UK
alec.muffett@uk.sun.com
[13] Dept. of Computer Science, Utrecht University,
P.O. Box 80089, 3508 TB Utrecht, The Netherlands
aardal@cs.uu.nl
[14] 59 Rangers Dr., Hudson, NH 03051, USA
craig.putnam@swift.mv.com

An Algorithm for Solving the Discrete Log Problem on Hyperelliptic Curves

Pierrick Gaudry[*]

LIX, École Polytechnique,
91128 Palaiseau Cedex, France
gaudry@lix.polytechnique.fr

[*] This work was supported by Action COURBES of INRIA (action coopérative de la direction scientifique de l'INRIA).

Analysis and Optimization of the TWINKLE Factoring Device

Arjen K. Lenstra[1] and Adi Shamir[2]

[1] Citibank, N.A., 1 North Gate Road, Mendham, NJ 07945-3104, U.S.A.,
`arjen.lenstra@citicorp.com`

[2] Computer Science Department, The Weizmann Institute, Rehovot 76100, Israel,
`shamir@wisdom.weizmann.ac.il`

Noisy Polynomial Interpolation and Noisy Chinese Remaindering

Daniel Bleichenbacher[1] and Phong Q. Nguyen[2]

[1] Bell Laboratories, Rm. 2A-366, 700 Mountain Av
Murray Hill, NJ 07974-0636, USA
bleichen@bell-labs.com and http://www.bell-labs.com/user/bleichen/
[2] École Normale Supérieure, Département d'Informatique,
45 rue d'Ulm, 75005 Paris, France
pnguyen@ens.fr and http://www.di.ens.fr/~pnguyen/

A Chosen Messages Attack on the ISO/IEC 9796–1 Signature Scheme

François Grieu

Innovatron, 1 rue Danton, 75006 Paris, France
fgrieu@innovatron.fr

Cryptanalysis of Countermeasures Proposed for Repairing ISO 9796-1

Marc Girault and Jean-François Misarsky

France Télécom - CNET
42 rue des Coutures, B.P. 6243
14066 CAEN CEDEX 4, FRANCE
{marc.girault, jeanfrancois.misarsky}@cnet.francetelecom.fr

Security Analysis of the Gennaro-Halevi-Rabin Signature Scheme

Jean-Sébastien Coron and David Naccache

Jean-Sébastien Coron

Ecole Normale Supérieure
45 rue d'Ulm
Paris, F-75230, France
coron@clipper.ens.fr

David Naccache

Gemplus Card International
34 rue Guynemer
Issy-les-Moulineaux, F-92447, France
david.naccache@gemplus.com

On the Security of 3GPP Networks

Michael Walker

Vodafone Airtouch and Royal Holloway College, University of London

One-Way Trapdoor Permutations Are Sufficient for Non-trivial Single-Server Private Information Retrieval

Eyal Kushilevitz[1] and Rafail Ostrovsky[2]

[1] IBM T.J. Watson Research Center, New-York and Computer Science Department,
Technion, Haifa 32000, Israel.
eyalk@cs.technion.ac.il, eyalk@watson.ibm.com

[2] Telcordia Technologies Inc., 445 South Street, Morristown, New Jersey 07960-6438,
USA
rafail@research.telcordia.com

Single Database Private Information Retrieval Implies Oblivious Transfer

Giovanni Di Crescenzo[1], Tal Malkin[2], and Rafail Ostrovsky[1]

[1] Telcordia Technologies, Inc., 445 South Street, Morristown, NJ, 07960.
E-mail: {giovanni,rafail}@research.telcordia.com.
[2] AT&T Labs – Research, 180 Park Ave., Florham Park, NJ, 07932.
E-mail: tal@research.att.com.
Work done at the Massachusetts Institute of Technology.

Authenticated Key Exchange Secure Against Dictionary Attacks

Mihir Bellare[1], David Pointcheval[2], and Phillip Rogaway[3]

[1] Dept. of Computer Science & Engineering, University of California at San Diego,
9500 Gilman Drive, La Jolla, CA 92093, USA, mihir@cs.ucsd.edu,
WWW home page: http://www-cse.ucsd.edu/users/mihir

[2] Dépt. d'Informatique–CNRS, École Normale Supérieure, 45 rue d'Ulm, 75230 Paris
Cedex 05, France, david.pointcheval@ens.fr,
WWW home page: http://www.dmi.ens.fr/~pointche

[3] Dept. of Computer Science, University of California at Davis,
Davis, CA 95616, USA, rogaway@cs.ucdavis.edu,
WWW home page: http://www.cs.ucdavis.edu/~rogaway

Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman

Victor Boyko[1], Philip MacKenzie[2], and Sarvar Patel[2]

[1] MIT Laboratory for Computer Science, boyko@theory.lcs.mit.edu
[2] Bell Laboratories, Lucent Technologies, {philmac, sarvar}@lucent.com

Fair Encryption of RSA Keys

Guillaume Poupard and Jacques Stern

École Normale Supérieure, Département d'informatique
45 rue d'Ulm, F-75230 Paris Cedex 05, France
email: {Guillaume.Poupard,Jacques.Stern}@ens.fr

Computing Inverses over a Shared Secret Modulus

Dario Catalano[1], Rosario Gennaro[2], and Shai Halevi[2]

[1] Dipartimento di Matematica e Informatica,
Università di Catania. Viale A. Doria 6, 95125 Catania.
Email: catalano@dmi.unict.it.
[2] IBM T.J.Watson Research Center,
PO Box 704, Yorktown Heights, New York 10598, USA.
Email: {rosario,shaih}@watson.ibm.com

Practical Threshold Signatures

Victor Shoup

IBM Zurich Research Lab, Säumerstr. 4, 8803 Rüschlikon, Switzerland
sho@zurich.ibm.com

Adaptively Secure Threshold Cryptography: Introducing Concurrency, Removing Erasures

Stanisław Jarecki and Anna Lysyanskaya

MIT Laboratory for Computer Science, Cambridge, MA 02139, USA
{stasio, anna}@theory.lcs.mit.edu

Confirmer Signature Schemes Secure against Adaptive Adversaries (Extended Abstract)

Jan Camenisch and Markus Michels

[1] IBM Research
Zurich Research Laboratory
CH–8803 Rüschlikon
jca@zurich.ibm.com
[2] Entrust Technologies (Switzerland)
Glatt Tower
CH–8301 Glattzentrum
Markus.Michels@entrust.com

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

Mihir Bellare[1], Alexandra Boldyreva[1], and Silvio Micali[2]

[1] Dept. of Computer Science & Engineering, University of California at San Diego,
9500 Gilman Drive, La Jolla, California 92093, USA.
E-mails: {mihir, aboldyre}@cs.ucsd.edu.
URLs: www-cse.ucsd.edu/users/{mihir, aboldyre}.

[2] MIT Laboratory for Computer Science,
545 Technology Square, Cambridge MA 02139, USA.

Using Hash Functions as a Hedge against Chosen Ciphertext Attack

Victor Shoup

IBM Zurich Research Lab, Säumerstr. 4, 8803 Rüschlikon, Switzerland
sho@zurich.ibm.com

Security Aspects of Practical Quantum Cryptography

Gilles Brassard[1], Norbert Lütkenhaus[2], Tal Mor[3,4], and Barry C. Sanders[5]

[1] Département IRO, Université de Montréal, C.P. 6128, succ. centre–ville,
Montréal (Québec), Canada H3C 3J7
brassard@iro.umontreal.ca

[2] Helsinki Institute of Physics, P.O.Box 9, 00014 Helsingin yliopisto, Finland
lutkenha@rock.helsinki.fi

[3] Electrical Engineering, College of Judea and Samaria, Ariel, Israel
talmo@cs.technion.ac.il

[4] Electrical Engineering, University of California at Los Angeles,
Los Angeles, CA 90095–1594, USA
talmo@ee.ucla.edu

[5] Department of Physics, Macquarie University, Sydney,
New South Wales 2109, Australia
barry.sanders@mq.edu.au

Perfectly Concealing Quantum Bit Commitment from any Quantum One-Way Permutation

Paul Dumais[1], Dominic Mayers[2], and Louis Salvail[3]

[1] Université de Montréal, Dept. of Computer Science, dumais@iro.umontreal.ca
[2] NEC Research Institute, Princeton, N-J, USA, mayers@research.nj.nec.com
[3] BRICS, Dept. of Computer Science,University of Århus, Århus, Denmark. salvail@brics.dk

General Secure Multi-Party Computation from any Linear Secret-Sharing Scheme

Ronald Cramer in Computer Science, Email: cramer@brics.dk,, Ivan Damgård ivan@daimi.aau.dk, and Ueli Maurer

Minimal-Latency Secure Function Evaluation

Donald Beaver

CertCo, Inc.

Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free

Ueli Maurer[1] and Stefan Wolf[1]

Computer Science Department, Swiss Federal Institute of Technology (ETH Zurich),
CH-8092 Zurich, Switzerland
{maurer,wolf}@inf.ethz.ch

New Attacks on PKCS#1 v1.5 Encryption

Jean-Sébastien Coron[1,3], Marc Joye[2], David Naccache[3], and Pascal Paillier[3]

[1] École Normale Supérieure
45 rue d'Ulm, 75005 Paris, France
coron@clipper.ens.fr
[2] Gemplus Card International
Parc d'Activités de Gémenos, B.P.100, 13881 Gémenos, France
marc.joye@gemplus.com
[3] Gemplus Card International
34 rue Guynemer, 92447 Issy-les-Moulineaux, France
{jean-sebastien.coron, david.naccache, pascal.paillier}@gemplus.com

A NICE Cryptanalysis

Éliane Jaulmes[1] and Antoine Joux[2]

[1] SCSSI, 18 rue du Docteur Zamenhof
F-92131 Issy-les-Moulineaux cedex, France
eliane.jaulmes@wanadoo.fr
[2] SCSSI, 18 rue du Docteur Zamenhof
F-92131 Issy-les-Moulineaux cedex, France
Antoine.Joux@ens.fr

Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations

Nicolas Courtois[1,3], Alexander Klimov[2], Jacques Patarin[3], and Adi Shamir[4]

[1] MS/LI, Toulon University, BP 132, F-83957 La Garde Cedex, France
courtois@univ-tln.fr

[2] Dept. of Appl. Math. & Cybernetics, Moscow State University, Moscow, Russia
ask@ispras.ru

[3] Bull CP8, 68, route de Versailles, BP45, 78431 Louveciennes Cedex, France
J.Patarin@frlv.bull.fr

[4] Dept. of Applied Math. The Weizmann Institute of Science, Rehovot 76100, Israel
shamir@wisdom.weizmann.ac.il

Cryptanalysis of Patarin's 2-Round Public Key System with S Boxes (2R)

Eli Biham

Computer Science Department
Technion – Israel Institute of Technology
Haifa 32000, Israel
Email: biham@cs.technion.ac.il
WWW: http://www.cs.technion.ac.il/∼biham/

Colossus and the German Lorenz Cipher – Code Breaking in WW II

Anthony E Sale, Hon. FBCS

Bletchley Park Trust
tsale@qufaro.demon.co.uk

Efficient Concurrent Zero-Knowledge in the Auxiliary String Model

Ivan Damgård

Aarhus University, BRICS

Efficient Proofs that a Committed Number Lies in an Interval

Fabrice Boudot

France Télécom - CNET
42 rue des Coutures, B.P. 6243
14066 CAEN CEDEX 4, FRANCE
`fabrice.boudot@cnet.francetelecom.fr`

A Composition Theorem for Universal One-Way Hash Functions

Victor Shoup

IBM Zurich Research Lab, Säumerstr. 4, 8803 Rüschlikon, Switzerland
sho@zurich.ibm.com

Exposure-Resilient Functions and All-Or-Nothing Transforms

Ran Canetti[1], Yevgeniy Dodis[2], Shai Halevi[1], Eyal Kushilevitz[3], and Amit Sahai[2]

[1] IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, New York 10598, USA. {canetti,shaih}@watson.ibm.com.

[2] Lab. for Computer Science, Massachusetts Institute of Technology, 545 Technology Square, Cambridge, MA 02149, USA. {yevgen,amits}@theory.lcs.mit.edu.

[3] IBM T.J. Watson Research Center and Department of Computer Science, Technion, Haifa 32000, Israel. eyalk@cs.technion.ac.il.

The Sum of PRPs is a Secure PRF

Stefan Lucks

Theoretische Informatik, Universität Mannheim
68131 Mannheim, Germany
lucks@th.informatik.uni-mannheim.de

Construction of Nonlinear Boolean Functions with Important Cryptographic Properties

Palash Sarkar[1] and Subhamoy Maitra[2]

[1] Applied Statistics Unit, Indian Statistical Institute,
203, B T Road, Calcutta 700 035, INDIA
palash@isical.ac.in

[2] Computer and Statistical Service Center, Indian Statistical Institute,
203, B T Road, Calcutta 700 035, INDIA
subho@isical.ac.in

Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions

Anne Canteaut[1], Claude Carlet[2], Pascale Charpin[1], and Caroline Fontaine[3]

[1] INRIA projet CODES
B.P. 105
78153 Le Chesnay Cedex - France.
{Anne.Canteaut,Pascale.Charpin}@inria.fr
[2] GREYC, Université de Caen
14032 Caen Cedex - France.
Claude.Carlet@info.unicaen.fr
[3] LIFL, Université des Sciences et Technologies de Lille
59655 Villeneuve d'Ascq Cedex - France.
Caroline.Fontaine@lifl.fr

Cox-Rower Architecture for Fast Parallel Montgomery Multiplication

Shinichi Kawamura[1], Masanobu Koike[2], Fumihiko Sano[2], and Atsushi Shimbo[1]

[1] Toshiba Research and Development Center
1, Komukai Toshiba-cho, Saiwai-ku, Kawasaki, 212-8582, Japan
[2] Toshiba System Integration Technology Center
3-22, Katamachi Fuchu-shi, Tokyo, 183-8512, Japan
{shinichi2.kawamura, masanobu2.koike, fumihiko.sano, atsushi.shimbo}
@toshiba.co.jp

Efficient Receipt-Free Voting Based on Homomorphic Encryption

Martin Hirt[1] and Kazue Sako[2]

[1] ETH Zurich, Switzerland, hirt@inf.ethz.ch
[2] NEC Corporation, Japan, sako@ccm.cl.nec.co.jp

How to Break a Practical MIX and Design a New One

Yvo Desmedt[1,2] and Kaoru Kurosawa[3]

[1] Department of Computer Science, Florida State University
PO Box 4530, 206 Love Building
Tallahassee, FL 32306-4530, USA
desmedt@cs.uwm.edu

[2] Dept. of Mathematics, Royal Holloway,
University of London, UK

[3] Dept. of Electrical and Electronic Engineering,
Faculty of Engineering, Tokyo Institute of Technology
2–12–1 O-okayama, Meguro-ku, Tokyo 152-8552, Japan
kurosawa@ss.titech.ac.jp

Improved Fast Correlation Attacks Using Parity-Check Equations of Weight 4 and 5

Anne Canteaut[1] and Michaël Trabbia[1,2]

[1] INRIA projet CODES
B.P. 105
78153 Le Chesnay Cedex - France
Anne.Canteaut@inria.fr
[2] Ecole Polytechnique
91128 Palaiseau Cedex - France
michael.trabbia@enst.fr

Advanced Slide Attacks

Alex Biryukov and David Wagner, Email: daw@cs.berkeley.edu