

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Antoine Joux (Ed.)

Advances in Cryptology – EUROCRYPT 2009

28th Annual International Conference on the Theory
and Applications of Cryptographic Techniques
Cologne, Germany, April 26-30, 2009
Proceedings

Volume Editor

Antoine Joux

DGA and University of Versailles Saint-Quentin-en-Yvelines

45, avenue des Etats-Unis, 78035 Versailles Cedex, France

E-mail: antoine.joux@m4x.org

Library of Congress Control Number: Applied for

CR Subject Classification (1998): E.3, F.2.1-2, G.2.1, D.4.6, K.6.5, C.2, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743

ISBN-10 3-642-01000-8 Springer Berlin Heidelberg New York

ISBN-13 978-3-642-01000-2 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

springer.com

© Springer-Verlag Berlin Heidelberg 2009

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper SPIN: 12648559 06/3180 5 4 3 2 1 0

*The original version of the book was revised:
The copyright line was incorrect. The Erratum
to the book is available at
DOI: [10.1007/978-3-642-01001-9_35](https://doi.org/10.1007/978-3-642-01001-9_35)*

Preface

You are holding the proceedings of Eurocrypt 2009, the 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques. This conference was organized by the International Association for Cryptologic Research in cooperation with the Horst Görtz Institute for IT-Security at the Ruhr-Universität Bochum. The local organization received additional support from several sponsors: Horst Görtz Stiftung, Deutsche Forschungsgemeinschaft, Bochum 2015, Secunet, NXP, IET, Taylor & Francis, AuthentiDate. The conference was held in Cologne, Germany.

The Eurocrypt 2009 Program Committee (PC) consisted of 29 members, listed on the next page. There were 148 submissions and 33 were selected to appear in this volume. Each submission was assigned to at least three PC members and reviewed anonymously. During the review process, the PC members were assisted by 131 external reviewers. Once the reviews were available, the committee discussed the papers in depth using the EasyChair conference management system. The authors of accepted papers were given five weeks to prepare the final versions included in these proceedings. The revised papers were not reviewed again and their authors bear the responsibility for their content.

In addition to the papers included in this volume, the conference also featured a Poster and a Rump session. The list of presented posters appears in this volume before the table of contents. Dan Bernstein served as the Chair of the Rump session. The conference also had the pleasure of hearing invited talks by Shafi Goldwasser and Phillip Rogaway.

The PC decided to give the Best Paper Award to Dennis Hofheinz and Eike Kiltz for their paper “Practical Chosen Ciphertext Secure Encryption from Factoring.” In addition, the PC selected two other papers for invitation to the *Journal of Cryptology*: “On Randomizing Some Hash Functions to Strengthen the Security of Digital Signatures” by Praveen Gauravaram and Lars Knudsen, and “Possibility and Impossibility Results for Encryption and Commitment Secure Under Selective Opening” by Mihir Bellare, Dennis Hofheinz and Scott Yilek.

I wish to thank all the people who contributed to this conference. First, all the authors who submitted their work. The PC members and their external reviewers for the thorough job they did while reading and commenting on the submissions. Without them, selecting the papers for this conference would have been an impossible task. I thank Andrei Voronkov for his review system EasyChair, I was especially impressed by the tools that helped me while assembling this volume. I am grateful to Arjen Lenstra for the help and advice he gave as representative of the IACR Board. I also would like to thank the General Chair Alexander May and his Co-chairs for making this conference possible.

Being the Program Chair for Eurocrypt 2009 was a great honor and I may only hope that the readers of these proceedings will find them as interesting as I found the task of selecting their content.

Organization

General Chair

Alexander May Ruhr-Universität Bochum, Germany

Co-chairs

Roberto Avanzi Christof Paar Ahmad Sadeghi
Jörg Schwenk Christopher Wolf

Program Chair

Antoine Joux DGA and Université de Versailles
 Saint-Quentin-en-Yvelines, France

Program Committee

Paulo Barreto University of São Paulo, Brazil
Alexandra Boldyreva Georgia Institute of Technology, USA
Colin Boyd Queensland University of Technology,
 Australia
Xavier Boyen Stanford University, USA
Mike Burmester Florida State University, USA
Serge Fehr CWI Amsterdam, The Netherlands
Marc Fischlin TU Darmstadt, Germany
Pierre-Alain Fouque École Normale Supérieure, Paris, France
Craig Gentry Stanford University, USA
Henri Gilbert Orange Labs, France (Eurocrypt 2010 Chair)
Helena Handschuh Spansion, France
Nick Howgrave-Graham NTRU Cryptosystems, USA
Thomas Johansson Lund University, Sweden
Jonathan Katz University of Maryland and IBM Research,
 USA
John Kelsey National Institute of Standards and
 Technology, USA
Kwangjo Kim Information and Communications University,
 Korea
Kaoru Kurosawa Ibaraki University, Japan
Reynald Lercier DGA/CELAR and Université de Rennes,
 France
Anna Lysyanskaya Brown University, USA
Rafail Ostrovsky University of California, Los Angeles, USA

Pascal Paillier	Gemalto Security Labs/Cryptography & Innovation, France
Duong Hieu Phan	Université de Paris 8, France
Christian Rechberger	IAIK, Graz University of Technology, Austria
Werner Schindler	Bundesamt für Sicherheit in der Informationstechnik, Germany
Thomas Shrimpton	Portland State University and University of Lugano, USA and Italy
Nigel Smart	University of Bristol, UK (Eurocrypt 2008 Chair)
Rainer Steinwandt	Florida Atlantic University, USA
Christine Swart	University of Cape Town, South Africa
Christopher Wolf	Ruhr University Bochum, Germany

External Reviewers

Abdalla, Michel	Gennaro, Rosario
Abe, Masayuki	Gonzalez, Juan
Andreeva, Elena	Goubin, Louis
Armknecht, Frederik	Gouget, Aline
Bangerter, Endre	Goyal, Vipul
Bellare, Mihir	van de Graaf, Jeroen
Benaloh, Josh	Halevi, Shai
Bernstein, Daniel J.	Hanaoka, Goichiro
Billet, Olivier	Hemenway, Brett
Bouillaguet, Charles	Heng, Swee Huay
Broker, Reinier	Herbst, Christoph
Brown, Dan	Herranz, Javier
Cash, David	Hisil, Huseyin
Chandran, Nishanth	Hoepfer, Katrin
Chen, Lidong	Hofheinz, Dennis
Chevallier-Mames, Benoît	Holz, Thorsten
Clavier, Christophe	Hutter, Michael
Cochran, Martin	Iorga, Michaela
Coron, Jean-Sébastien	Ishai, Yuval
Dent, Alex	Iwata, Tetsu
Dodis, Yevgeniy	Jacobson, Michael
Duc, Dang Nguyen	Jain, Abhishek
Fiore, Dario	Kiltz, Eike
Fischer, Jan	Koshihara, Takeshi
Furukawa, Jun	Krawczyk, Hugo
Galbraith, Steven D.	Kursawe, Klaus
Garay, Juan	Lamberger, Mario
Gazzoni Filho, Décio Luiz	Lange, Tanja
Gebhardt, Max	Lee, Younho

Lehmann, Anja
Lenstra, Arjen
Lindell, Yehuda
Lochter, Manfred
Lu, Steve
Lucks, Stefan
Lyubashevsky, Vadim
Margraf, Marian
Maximov, Alexander
Mendel, Florian
Montenegro, Jose
Moran, Tal
Morrissey, Paul
Moss, Andrew
Naccache, David
Nad, Tomislav
Naehrig, Michael
Namprempre, Chanathip
Neven, Gregory
Nguyen, Phong
Niedermeyer, Frank
Noack, Andreas
O'Neill, Adam
Ogata, Wakaha
Ohkubo, Miyako
Oliveira, Leonardo
Oswald, Elisabeth
Page, Dan
Pandey, Omkant
Paul, Souradyuti
Peikert, Chris
Perlner, Ray
Persiano, Giuseppe
Pietrzak, Krzysztof
Pointcheval, David
Poschmann, Axel
Preneel, Bart
Priemuth-Schmid, Deike
Quisquater, Jean-Jacques
Ramzan, Zulfikar
Rappe, Dörte
Regenscheid, Andrew
Rezaeian Farashahi, Reza
Ristenpart, Thomas
Rose, Greg
Sakane, Hirofumi
Schläffer, Martin
Schmidt, Jörn-Marc
Schoenmakers, Berry
Schröder, Dominique
Schulte-Geers, Ernst
Segev, Gil
Shacham, Hovav
Shparlinski, Igor
Spitz, Stefan
Stam, Martijn
Stein, Oliver
Steinberger, John
Szekely, Alexander
Tillich, Stefan
Toft, Tomas
Tuengerthal, Max
Tunstall, Michael
Van Assche, Gilles
Vercauteren, Frederik
Vergnaud, Damien
Visconti, Ivan
Warinschi, Bogdan
Waters, Brent
Wee, Hoeteck
Wolf, Stefan
Wyseur, Brecht
Yerukhimovich, Arkady
Zenner, Erik
Zimmer, Sébastien

List of Presented Posters

Physically Unclonable Pseudorandom Functions

*Frederik Armknecht, Ahmad-Reza Sadeghi, Pim Tuyls,
Roel Maes and Berk Sunar*

Automatic Generation of sound Zero-Knowledge Protocols

*Endre Bangerter, Jan Camenisch, Stephan Krenn,
Ahmad-Reza Sadeghi and Thomas Schneider*

On the Data Complexity of Statistical Attacks Against Block Ciphers

Céline Blondeau and Benoît Gérard

Anonymity from Asymmetry: New Constructions for Anonymous HIBE

Dan Boneh and Léo Ducas

Pairing with Supersingular Trace Zero Varieties Revisited

Emanuele Cesena

Odd-Char Multivariate Hidden Field Equations

*Ming-Shing Chen, Jintai Ding, Chia-Hsin Owen Chen,
Fabian Werner and Bo-Yin Yang*

Finding Good Linear Approximations of Block Ciphers and its
Application to Cryptanalysis of Reduced Round DES

Rafaël Fourquet, Pierre Loidreau and Cédric Tavernier

Techniques for Public Key Cryptographic Acceleration on Graphics Processors

Owen Harrison and John Waldron

Statistical Tests for Key Recovery Using Multidimensional Extension
of Matsui's Algorithm 1

Miia Hermelin, Joo Yeon Cho and Kaisa Nyberg

The Key-Dependent Attack on Block Ciphers

Xiaorui Sun and Xuejia Lai

On Privacy Losses in the Trusted Agent Model

Paulo Mateus and Serge Vaudenay

Solving Low-Complexity Ciphers with Optimized SAT Solvers

Karsten Nohl and Mate Soos

A Geometric Approach on Pairings and Hierarchical Predicate Encryption.

Tatsuaki Okamoto and Katsuyuki Takashima

Generic Attacks on Feistel Networks with Internal Permutations
Jacques Patarin and Joana Treger

A Formal Treatment of Range Test of a Discrete Logarithm through Revealing
of a Monotone Function — Conditions, Limitations and Misuse
Kun Peng and Bao Feng

Could The 1-MSB Input Difference Be The Fastest Collision Attack For MD5?
Tao Xie, Dengguo Feng and Fanbao Liu

Table of Contents

Security, Proofs and Models (1)

Possibility and Impossibility Results for Encryption and Commitment Secure under Selective Opening	1
<i>Mihir Bellare, Dennis Hofheinz, and Scott Yilek</i>	
Breaking RSA Generically Is Equivalent to Factoring	36
<i>Divesh Aggarwal and Ueli Maurer</i>	
Resettably Secure Computation	54
<i>Vipul Goyal and Amit Sahai</i>	
On the Security Loss in Cryptographic Reductions	72
<i>Chi-Jen Lu</i>	

Hash Cryptanalysis

On Randomizing Hash Functions to Strengthen the Security of Digital Signatures	88
<i>Praveen Gauravaram and Lars R. Knudsen</i>	
Cryptanalysis of MDC-2	106
<i>Lars R. Knudsen, Florian Mendel, Christian Rechberger, and Søren S. Thomsen</i>	
Cryptanalysis on HMAC/NMAC-MD5 and MD5-MAC	121
<i>Xiaoyun Wang, Hongbo Yu, Wei Wang, Haina Zhang, and Tao Zhan</i>	
Finding Preimages in Full MD5 Faster Than Exhaustive Search	134
<i>Yu Sasaki and Kazumaro Aoki</i>	

Group and Broadcast Encryption

Asymmetric Group Key Agreement	153
<i>Qianhong Wu, Yi Mu, Willy Susilo, Bo Qin, and Josep Domingo-Ferrer</i>	
Adaptive Security in Broadcast Encryption Systems (with Short Ciphertexts)	171
<i>Craig Gentry and Brent Waters</i>	
Traitors Collaborating in Public: Pirates 2.0	189
<i>Olivier Billet and Duong Hieu Phan</i>	

Cryptosystems (1)

Key Agreement from Close Secrets over Unsecured Channels	206
<i>Bhavana Kanukurthi and Leonid Reyzin</i>	
Order-Preserving Symmetric Encryption	224
<i>Alexandra Boldyreva, Nathan Chenette, Younho Lee, and Adam O'Neill</i>	
A Double-Piped Mode of Operation for MACs, PRFs and PROs: Security beyond the Birthday Barrier	242
<i>Kan Yasuda</i>	

Cryptanalysis

On the Security of Cryptosystems with Quadratic Decryption: The Nicest Cryptanalysis	260
<i>Guilhem Castagnos and Fabien Laguillaumie</i>	
Cube Attacks on Tweakable Black Box Polynomials	278
<i>Itai Dinur and Adi Shamir</i>	
Smashing SQUASH-0	300
<i>Khaled Ouafi and Serge Vaudenay</i>	

Cryptosystems (2)

Practical Chosen Ciphertext Secure Encryption from Factoring	313
<i>Dennis Hofheinz and Eike Kiltz</i>	
Realizing Hash-and-Sign Signatures under Standard Assumptions	333
<i>Susan Hohenberger and Brent Waters</i>	
A Public Key Encryption Scheme Secure against Key Dependent Chosen Plaintext and Adaptive Chosen Ciphertext Attacks	351
<i>Jan Camenisch, Nishanth Chandran, and Victor Shoup</i>	

Invited Talk

Cryptography without (Hardly Any) Secrets ?	369
<i>Shafi Goldwasser</i>	

Security, Proofs and Models (2)

Salvaging Merkle-Damgård for Practical Applications	371
<i>Yevgeniy Dodis, Thomas Ristenpart, and Thomas Shrimpton</i>	

On the Security of Padding-Based Encryption Schemes - or – Why We Cannot Prove OAEP Secure in the Standard Model	389
<i>Eike Kiltz and Krzysztof Pietrzak</i>	
Simulation without the Artificial Abort: Simplified Proof and Improved Concrete Security for Waters' IBE Scheme	407
<i>Mihir Bellare and Thomas Ristenpart</i>	
On the Portability of Generalized Schnorr Proofs	425
<i>Jan Camenisch, Aggelos Kiayias, and Moti Yung</i>	
Side Channels	
A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks	443
<i>François-Xavier Standaert, Tal G. Malkin, and Moti Yung</i>	
A Leakage-Resilient Mode of Operation	462
<i>Krzysztof Pietrzak</i>	
Curves	
ECM on Graphics Cards	483
<i>Daniel J. Bernstein, Tien-Ren Chen, Chen-Mou Cheng, Tanja Lange, and Bo-Yin Yang</i>	
Double-Base Number System for Multi-scalar Multiplications	502
<i>Christophe Doche, David R. Kohel, and Francesco Sica</i>	
Endomorphisms for Faster Elliptic Curve Cryptography on a Large Class of Curves	518
<i>Steven D. Galbraith, Xibin Lin, and Michael Scott</i>	
Generating Genus Two Hyperelliptic Curves over Large Characteristic Finite Fields	536
<i>Takakazu Satoh</i>	
Randomness	
Verifiable Random Functions from Identity-Based Key Encapsulation	554
<i>Michel Abdalla, Dario Catalano, and Dario Fiore</i>	
Optimal Randomness Extraction from a Diffie-Hellman Element	572
<i>Céline Chevalier, Pierre-Alain Fouque, David Pointcheval, and Sébastien Zimmer</i>	
A New Randomness Extraction Paradigm for Hybrid Encryption	590
<i>Eike Kiltz, Krzysztof Pietrzak, Martijn Stam, and Moti Yung</i>	
Erratum to: Advances in Cryptology – EUROCRYPT 2009	E1
<i>Antoine Joux</i>	
Author Index	611