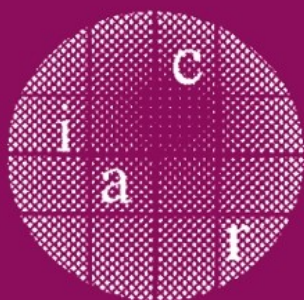


Eli Biham (Ed.)

LNCS 2656

# Advances in Cryptology – EUROCRYPT 2003

International Conference on the Theory  
and Applications of Cryptographic Techniques  
Warsaw, Poland, May 2003, Proceedings



Springer

# Lecture Notes in Computer Science

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

2656

**Springer**

*Berlin*

*Heidelberg*

*New York*

*Barcelona*

*Hong Kong*

*London*

*Milan*

*Paris*

*Tokyo*

Eli Biham (Ed.)

# Advances in Cryptology – EUROCRYPT 2003

International Conference on the Theory  
and Applications of Cryptographic Techniques  
Warsaw, Poland, May 4-8, 2003  
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany  
Juris Hartmanis, Cornell University, NY, USA  
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Eli Biham  
Technion - Israel Institute of Technology  
Computer Science Department  
Haifa 32000, Israel  
E-mail: biham@cs.technion.ac.il

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek  
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;  
detailed bibliographic data is available in the Internet at <<http://dnb.ddb.de>>.

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

ISSN 0302-9743

ISBN 3-540-14039-5 Springer-Verlag 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-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York  
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© International Association for Cryptologic Research 2003  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin GmbH  
Printed on acid-free paper SPIN: 10928608 06/3142 5 4 3 2 1 0

# Preface

These are the proceedings of EUROCRYPT 2003, the 22nd annual EUROCRYPT conference. The conference was sponsored by the IACR, the International Association for Cryptologic Research, [www.iacr.org](http://www.iacr.org), this year in cooperation with the Institute of Mathematics and Cryptology, Faculty of Cybernetics, Military University of Technology, Warsaw, Poland. The General Chair, Jerzy Gawinecki, was responsible for the local organization, and the conference registration was handled by the IACR secretariat at the University of California, Santa Barbara, USA.

A total of 37 papers were accepted for presentation at the conference, out of 156 papers submitted (of which one was withdrawn by the authors shortly after the submission deadline). These proceedings contain revised versions of the accepted papers. In addition two invited talks were given: the first was given by Kris Gaj and Arkadiusz Orłowski, entitled “Facts and Myths of Enigma: Breaking Stereotypes.” The second invited talk was given by Jacques Stern entitled “Why Provable Security Matters?” The conference program also included a rump session, chaired by Stanisław Jarecki, which featured short informal talks on recent results.

The reviewing process was a challenging task, and many good submissions had to be rejected. Each paper was reviewed by at least three members of the program committee, and papers co-authored by a member of the program committee were reviewed by at least six (other) members. The reviews were then followed by deep discussions on the papers, which contributed a lot to the quality of the final selection. In most cases, extensive comments were sent to the authors. It was a pleasure for me to work with the program committee, whose members worked very hard over several months. I am also very grateful to the external referees who contributed with their special expertise to the selection process. Their work is highly appreciated.

The submission of papers was done using an electronic submission software written by Chanathip Namprempre for CRYPTO 2000 with modifications developed by Andre Adelsbach for EUROCRYPT 2001. All but two papers were submitted using this software, while the two others were submitted on paper and then scanned and entered into the software. During the review process, the program committee was mainly communicating using a review software written by Bart Preneel, Wim Moreau, and Joris Claessens for EUROCRYPT 2000. I would like to thank Orr Dunkelman and Julia Stolin for their help in installing, solving problems, and adding features to the software. I am also very grateful to Wim Moreau for his great help in solving some of the problems we had with the software. The final decisions were made during a committee meeting in Paris. I would like to thank Helena Handschuh and Gemplus for organizing and hosting the meeting. I would also like to acknowledge Elad Barkan and Pnina Cohen for their help whenever it was required.

On behalf of the General Chair I would like to acknowledge the members of the local organizing committee in Warsaw. For financial support of the conference we are very grateful to this year's sponsors.

It is my pleasure to thank the General Chair, Prof. Jerzy Gawinecki, for all his work in organizing the conference, and for the pleasant collaboration and various pieces of advice. I know he spent a lot of effort, during a period of over two years, organizing the conference.

Finally, but most importantly, I would like to thank all the authors from all over the world who submitted papers to the conference, and all the participants at the conference.

February 2003

Eli Biham

# EUROCRYPT 2003

May 4–8, 2003, Warsaw, Poland

Sponsored by the

*International Association for Cryptologic Research (IACR)*

in cooperation with the

*Institute of Mathematics and Cryptology, Faculty of Cybernetics,  
Military University of Technology, Warsaw*

## General Chair

Jerzy Gawinecki, Institute of Mathematics and Cryptology,  
Faculty of Cybernetics, Military University of Technology,  
Kaliskiego Str. 2, 00-908 Warsaw, Poland

## Program Chair

Eli Biham, Computer Science Department, Technion, Israel  
Institute of Technology, Technion City, Haifa 32000, Israel

## Program Committee

Johannes Buchmann ..... TU Darmstadt, Germany  
Christian Cachin ..... IBM Research, Switzerland  
Don Coppersmith ..... IBM Research, USA  
Ronald Cramer ..... Aarhus, Denmark  
Joan Daemen ..... Protonworld, Belgium  
Yevgeniy Dodis ..... New York University, USA  
Cynthia Dwork ..... Microsoft, USA  
Juan Garay ..... Bell Labs, USA  
Helena Handschuh ..... Gemplus, France  
Stanisław Jarecki ..... Stanford, USA  
Kwangjo Kim ..... ICU, Korea  
Lars R. Knudsen ..... Technical University of Denmark  
Shiho Moriai ..... NTT, Japan  
Moni Naor ..... Weizmann Institute of Science, Israel  
Paul Van Oorschot ..... Carleton University, Canada  
Josef Pieprzyk ..... Macquarie University, Australia  
David Pointcheval ..... CNRS–ENS, France  
Matt Robshaw ..... Royal Holloway, UK  
Berry Schoenmakers ..... TU Eindhoven, The Netherlands  
Nigel Smart ..... University of Bristol, UK  
Douglas R. Stinson ..... Waterloo, Canada  
Serge Vaudenay ..... EPFL, Switzerland



## Local Organizing Committee

Andrzej Ameljańczyk	Tomasz Korza	Marek Niezgótka
Grażyna Biernacka	Zenon Kosowski	Roman Oziębała
Bogdan Bojarski	Ryszard Kossowski	Jacek Papaj
Piotr Bora	Krzysztof Mańk	Janusz Szmidt
Marek Dukaczewski	Maciej Mączyński	Arkadiusz Szymaniec
Anna Gajownik	Dobrosław Mąka	Aleksander Wittlin
Stanisław Janeczko	Bogdan Miszczak	
Tomasz Kijko	Michał Misztal	

## Sponsors

### Gold Sponsors

Comp S.A., Warsaw, Poland

Microsoft Corporation, Redmond, WA, USA

### Silver Sponsors

Radomska Wytwórnia Telefonów, “Telefony Polskie” S.A., Radom, Poland

### Bronze Sponsors

Military Communication Institute, Zegrze, Poland

Telecommunications Research Institute, Warsaw, Poland

Enigma Systemy Ochrony Informacji Sp. z o.o., Warsaw, Poland

## External Referees

Masayuki Abe	David Divincenzo	Danny Harnik
Kazumaro Aoki	Jeroen Doumen	Birgit Henhapl
Gildas Avoine	Orr Dunkelman	Florian Hess
Michael Backes	Nelly Fazio	Deukjo Hong
Harad Baier	Matthias Fitzi	Fumitaka Hoshino
Boaz Barak	Pierre-Alain Fouque	Nick Howgrave-Graham
Alexander Barg	Eiichiro Fujisaki	Yuval Ishai
Elad Barkan	Steven Galbraith	Oleg Izmerly
Josh Benaloh	David Gamarnik	Antoine Joux
Simon Blackburn	Katherina Geissler	Pascal Junod
Daniel Bleichenbacher	Rosario Gennaro	Mads Jurik
Dan Boneh	Yael Gertner	Mike Just
Emmanuel Bresson	Henri Gilbert	Masayuki Kanda
Jan Camenisch	Bobi Gilburd	Nathan Keller
Ran Canetti	Eu-Jin Goh	Svein Knapskog
Brice Canvel	Jovan Golić	Tetsutaro Kobayashi
Dario Catalano	Philippe Golle	Evangelos Kranakis
Olivier Chevassut	Louis Granboulan	Hugo Krawczyk
Jean-Sébastien Coron	Jens Groth	Michiharu Kudo
Alex Dent	Stuart Haber	Byoungcheon Lee
Jean-François Dhem	Shai Halevi	Yehuda Lindell

Yi Lu	Francis Olivier	Gregory Sorkin
Christof Ludwig	Dan Page	Jessica Staddon
Phil MacKenzie	Pascal Paillier	Martijn Stam
Tal Malkin	Matthew Parker	Michael Steiner
John Malone-Lee	Kenny Paterson	Jacques Stern
Wenbo Mao	Benny Pinkas	Koutarou Suzuki
Keith Martin	Guillaume Poupard	Tsuyoshi Takagi
Gwenaëlle Martinet	Bart Preneel	Barbara Terhal
Willi Meier	Haavard Raddum	Yuuki Tokunaga
Marine Minier	Omer Reingold	Pim Tuyls
Ilya Mironov	Leonid Reyzin	Christophe Tymen
Bodo Moeller	Alon Rosen	Frederik Vercauteren
Jean Monnerat	Louis Salvail	Ullrich Vollmer
Tal Mor	Arthur Schmidt	Huaxiong Wang
Sean Murphy	Hovav Shaham	Michael Wiener
Phong Nguyen	Igor Shparlinski	Fangguo Zhang
Antonio Nicolosi	Hervé Sibert	Xianmo Zhang
Roberto Oliveira	Adam Smith	

# Table of Contents

## Cryptanalysis I

Cryptanalysis of the EMD Mode of Operation . . . . .	1
<i>Antoine Joux</i>	
On the Optimality of Linear, Differential, and Sequential Distinguishers . . . . .	17
<i>Pascal Junod</i>	
A Toolbox for Cryptanalysis: Linear and Affine Equivalence Algorithms . . . . .	33
<i>Alex Biryukov, Christophe De Cannière, An Braeken, Bart Preneel</i>	

## Secure Multi-party Computation I

Two-Threshold Broadcast and Detectable Multi-party Computation . . . . .	51
<i>Matthias Fitzi, Martin Hirt, Thomas Holenstein, Jürg Wullschleger</i>	
On the Limitations of Universally Composable Two-Party Computation without Set-up Assumptions . . . . .	68
<i>Ran Canetti, Eyal Kushilevitz, Yehuda Lindell</i>	
Fair Secure Two-Party Computation . . . . .	87
<i>Benny Pinkas</i>	

## Invited Talk I

Facts and Myths of Enigma: Breaking Stereotypes . . . . .	106
<i>Kris Gaj, Arkadiusz Orłowski</i>	

## Zero-Knowledge Protocols

Resettable Zero-Knowledge in the Weak Public-Key Model . . . . .	123
<i>Yunlei Zhao, Xiaotie Deng, C.H. Lee, Hong Zhu</i>	
Simulatable Commitments and Efficient Concurrent Zero-Knowledge . . . . .	140
<i>Daniele Micciancio, Erez Petrank</i>	
Simulation in Quasi-Polynomial Time, and Its Application to Protocol Composition . . . . .	160
<i>Rafael Pass</i>	

Strengthening Zero-Knowledge Protocols Using Signatures ..... 177  
*Juan A. Garay, Philip MacKenzie, Ke Yang*

**Foundations and Complexity Theoretic Security**

Nearly One-Sided Tests and the Goldreich-Levin Predicate ..... 195  
*Gustav Hast*

Efficient and Non-malleable Proofs of Plaintext Knowledge and Applications ..... 211  
*Jonathan Katz*

**Public Key Encryption**

A Public Key Encryption Scheme Based on the Polynomial Reconstruction Problem ..... 229  
*Daniel Augot, Matthieu Finiasz*

A Simpler Construction of CCA2-Secure Public-Key Encryption under General Assumptions ..... 241  
*Yehuda Lindell*

A Forward-Secure Public-Key Encryption Scheme ..... 255  
*Ran Canetti, Shai Halevi, Jonathan Katz*

Certificate-Based Encryption and the Certificate Revocation Problem.... 272  
*Craig Gentry*

**New Primitives**

CAPTCHA: Using Hard AI Problems for Security ..... 294  
*Luis von Ahn, Manuel Blum, Nicholas J. Hopper, John Langford*

Concealment and Its Applications to Authenticated Encryption ..... 312  
*Yevgeniy Dodis, Jee Hea An*

**Cryptanalysis II**

Predicting the Shrinking Generator with Fixed Connections ..... 330  
*Patrik Ekdahl, Willi Meier, Thomas Johansson*

Algebraic Attacks on Stream Ciphers with Linear Feedback ..... 345  
*Nicolas T. Courtois, Willi Meier*

**Elliptic Curves Cryptography**

Counting Points on Elliptic Curves over Finite Fields of Small Characteristic in Quasi Quadratic Time ..... 360  
*Reynald Lercier, David Lubicz*

The GHS Attack Revisited .....	374
<i>Florian Hess</i>	

Improved Algorithms for Efficient Arithmetic on Elliptic Curves Using Fast Endomorphisms .....	388
<i>Mathieu Ciet, Tanja Lange, Francesco Sica, Jean-Jacques Quisquater</i>	

## Digital Signatures

A Signature Scheme as Secure as the Diffie-Hellman Problem .....	401
<i>Eu-Jin Goh, Stanisław Jarecki</i>	

Aggregate and Verifiably Encrypted Signatures from Bilinear Maps .....	416
<i>Dan Boneh, Craig Gentry, Ben Lynn, Hovav Shacham</i>	

Hypercubic Lattice Reduction and Analysis of GGH and NTRU Signatures .....	433
<i>Michael Szydło</i>	

## Invited Talk II

Why Provable Security Matters? .....	449
<i>Jacques Stern</i>	

## Cryptanalysis III

On the Security of RDSA .....	462
<i>Pierre-Alain Fouque, Guillaume Poupard</i>	

Cryptanalysis of the Public-Key Encryption Based on Braid Groups .....	477
<i>Eonkyung Lee, Je Hong Park</i>	

A Theoretical Treatment of Related-Key Attacks: RKA-PRPs, RKA-PRFs, and Applications .....	491
<i>Mihir Bellare, Tadayoshi Kohno</i>	

## Key Exchange

Provably Secure Threshold Password-Authenticated Key Exchange .....	507
<i>Mario Di Raimondo, Rosario Gennaro</i>	

A Framework for Password-Based Authenticated Key Exchange .....	524
<i>Rosario Gennaro, Yehuda Lindell</i>	

## Information Theoretic Cryptography

The Security of Many-Round Luby-Rackoff Pseudo-Random Permutations .....	544
<i>Ueli Maurer, Krzysztof Pietrzak</i>	

New Bounds in Secret-Key Agreement: The Gap between Formation  
and Secrecy Extraction . . . . . 562  
*Renato Renner, Stefan Wolf*

**Secure Multi-party Computation II**

Round Efficiency of Multi-party Computation with a Dishonest  
Majority . . . . . 578  
*Jonathan Katz, Rafail Ostrovsky, Adam Smith*

Efficient Multi-party Computation over Rings . . . . . 596  
*Ronald Cramer, Serge Fehr, Yuval Ishai, Eyal Kushilevitz*

**Group Signatures**

Foundations of Group Signatures: Formal Definitions, Simplified  
Requirements, and a Construction Based on General Assumptions . . . . . 614  
*Mihir Bellare, Daniele Micciancio, Bogdan Warinschi*

Extracting Group Signatures from Traitor Tracing Schemes . . . . . 630  
*Aggelos Kiayias, Moti Yung*

**Author Index** . . . . . 649

# Cryptanalysis of the EMD Mode of Operation

Antoine Joux

DCSSI Crypto Lab  
51, Bd de Latour-Maubourg  
75700 PARIS 07 SP  
FRANCE  
antoine.joux@m4x.org

**Abstract.** In this paper, we study the security of the Encrypt-Mask-Decrypt mode of operation, also called EMD, which was recently proposed for applications such as disk-sector encryption. The EMD mode transforms an ordinary block cipher operating on  $n$ -bit blocks into a tweakable block cipher operating on large blocks of size  $nm$  bits. We first show that EMD is not a secure tweakable block cipher and then describe efficient attacks in the context of disk-sector encryption. We note that the parallelizable variant of EMD, called EME that was proposed at the same time is also subject to these attacks.

In the course of developing one of the attacks, we revisit Wagner's generalized birthday algorithm and show that in some special cases it performs much more efficiently than in the general case. Due to the large scope of applicability of this algorithm, even when restricted to these special cases, we believe that this result is of independent interest.

## 1 Introduction

Very recently, Rogaway proposed in [5] two new modes of operation that are specifically tailored for applications such as disk-sector encryption. The first mode called EMD (Encrypt-Mask-Decrypt) mostly consists in two consecutive passes of CBC encryption/decryption. Thus it is a sequential mode. The second mode called EME is a parallelizable version of EMD. In an updated version of [5], written with Halevi, the EMD algorithm is presented under the new name CMC. In particular, during the First IEEE International Security in Storage Workshop, held Dec. 11th, 2002 in Greenbelt, Maryland, the algorithm was presented under this new name.

In order to encrypt disk-sectors, several important properties are often required. First, when encrypting a single sector, a change in any single plaintext bit should impact the complete ciphertext sector. Since disk sectors are much larger than the block-size of usual block ciphers and since ordinary modes of operation such a CBC encryption do not ensure this property, this requirement calls for a specific construction. Second, for efficiency reasons, each sector should be encrypted independently of other sectors. As a consequence, an electronic code book at the sector level is expected. However, to avoid attacks based on sectors

switching, it is highly desirable to use a (slightly) different encryption for each sector. This idea can be rigorously realized by using the notion of tweakable block ciphers which was recently proposed by Liskov, Rivest and Wagner in [4]. Informally, a tweakable block cipher is a block cipher which possesses an extra input called the tweak. It should resist distinguishing attacks mounted by powerful adversaries which are allowed access to encryption and decryption oracles and can choose both the plaintext or ciphertext messages and the tweak parameters.

In order to meet these specifications, Rogaway proposed the modes of operation EMD and EME in order to build a tweakable block cipher with a large blocksize of  $nm$  bits from an ordinary block cipher with a blocksize of  $n$  bits. In these constructions,  $m$  represents the number of blocks that can be fitted into a single disk sector. In [5], he also stated a security theorem for the EMD mode

In this paper, we show that neither the EMD nor the EME modes of operation are secure tweakable block cipher. We proceed in several steps, first in section 2 we briefly recall the constructions from [5], then in section 3 we describe distinguishing attacks against the two modes, finally in section 4 we show practical attacks in the context of disk-sector encryption. In one of the practical attacks we make use of Wagner’s algorithm for solving the generalized birthday problem, which he introduced at Crypto’2002 in [6]. In order to improve the attack, we need to use the algorithm in a special case which was not considered by Wagner. It turns out that in this special case, the algorithm still works and moreover it becomes much more efficient than in the general case. An heuristic analysis of Wagner’s algorithm restricted to these special cases is given in appendix.

## 2 Description of EMD and EME

In this section, we give brief descriptions of the EMD and EME modes of operation as proposed in [5]. We only describe the forward direction (encryption). For complete specifications, the reader should refer to the original paper [5].

### 2.1 The EMD Mode

The EMD (Encrypt-Mask-Decrypt) mode of operation is based on CBC encryption. In order to simplify the description of this mode, we use two subroutines `CBCEncrypt` and `CBCDecrypt` that respectively perform CBC encryption and CBC decryption. These routines take as input a keyed block cipher  $E_K$  and a  $m$ -uple of input blocks  $X_1, \dots, X_m$  and output a  $m$ -uple  $Y_1, Y_2, \dots, Y_m$ . There is a simple but important difference between ordinary CBC decryption and the CBC decryption as used in EMD. More precisely, in the latter case, individual blocks are encrypted (by the block cipher  $E_K$ ) instead of being decrypted (by its inverse  $E_K^{-1}$ ). The two routines `CBCEncrypt` and `CBCDecrypt` are respectively described in tables 1 and 2.