

# Lecture Notes in Computer Science

950

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

Advisory Board: W. Brauer D. Gries J. Stoer

Alfredo De Santis (Ed.)

# Advances in Cryptology – EUROCRYPT '94

Workshop on the Theory and Application  
of Cryptographic Techniques  
Perugia, Italy, May 9-12, 1994  
Proceedings



Springer

Series Editors

Gerhard Goos  
Universität Karlsruhe  
Vincenz-Priessnitz-Straße 3, D-76128 Karlsruhe, Germany

Juris Hartmanis  
Department of Computer Science, Cornell University  
4130 Upson Hall, Ithaca, NY 14853, USA

Jan van Leeuwen  
Department of Computer Science, Utrecht University  
Padualaan 14, 3584 CH Utrecht, The Netherlands

Volume Editor

Alfredo De Santis  
Dipartimento di Informatica ed Applicazioni, Università di Salerno  
I-84081 Baronissi, Italy

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

**Advances in cryptology : proceedings / EUROCRYPT '94,  
Workshop on the Theory and Application of Cryptographic  
Techniques, Perugia, Italy, May 9 - 12, 1994. Alfredo DeSantis  
(ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ;  
Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 1995  
(Lecture notes in computer science ; 950)  
ISBN 3-540-60176-7**

NE: DeSantis, Alfredo [Hrsg.]; EUROCRYPT <12, 1994, Perugia>; GT

CR Subject Classification (1991): E.3-4, G.2.1, D.4.6, F.2.1-2, C.2, J.1

ISBN 3-540-60176-7 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 1995  
Printed in Germany

Typesetting: Camera-ready by author  
SPIN 10486452 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

## Preface

Eurocrypt is a series of open workshops devoted to all aspects of cryptologic research, both theoretical and practical. The first workshop was held in 1982, and since then the meetings have taken place in various places in Europe. The Eurocrypt meetings and the Crypto meetings in Santa Barbara, California, are sponsored by the International Association for Cryptologic Research (IACR).

Eurocrypt 94 was held on May 9–12, 1994, in Perugia, an Italian city that was a city-state of Etruria in the 7th and 6th centuries BC. It is a pleasure to thank the general chair William Wolfowitz and the organizing committee, who all contributed to make a well organized and successful conference.

There were 137 submitted papers which were considered by the Program Committee. Of these, 2 were withdrawn and 36 were selected for presentation and publication in the proceedings. Two of the papers appearing in the proceedings are merged papers from two submissions. These proceedings contain revised versions of the 36 contributed talks. Each paper was sent to at least 3 members of the Program Committee for comments. Revisions were not checked on their scientific aspects. Some authors will write final versions of their papers for publication in refereed journals. Of course the authors bear full responsibility for the contents of their papers.

Silvio Micali, MIT, gave a brilliant invited talk on the Clipper Chip and Fair Cryptosystems.

I am very grateful to the 11 members of the Program Committee for their hard work and the difficult task of selecting about 38% of the submitted papers. As usual, submissions to Eurocrypt 94 were required to be anonymous. The more recent tradition that a Program Committee member can be the author of at most one accepted paper has been followed. Papers submitted by members of the Program Committee were sent to all other members. The entire refereeing process was done by electronic mail.

The following referees and external experts helped the Program Committee in reaching their decisions: S. R. Blackburn, Carlo Blundo, S. Boucheron, Gilles Brassard, Odoardo Brugia, Marco Bucci, Mike Burmester, Claude Carlet, Pascale Charpin, Jean-Marc Couveignes, Denes, Giovanni Di Crescenzo, Michele Elia, Piero Filippini, Toru Fujiwara, Marc Girault, Akira Hayashi, Toshiya Itoh, Hugo Krawczyk, Kaoru Kurosawa, Antoine Joux, James Massey, Mitsuru Matsui, Tsutomu Matsumoto, Natsume Matsuzaki, Renato Menicocci, Chris Mitchell, Atsuko Miyaji, Emilio Montolivo, Francois Morain, David M'raihi,

Sean Murphy, Giuseppe Persiano, Jean-Marc Piveteau, G. M. Poscetti, Jean-Jacques Quisquater, Kouichi Sakurai, Miklos Santha, Nicolas Sendrier, Matteo Sereno, Hiroki Shizuya, Dan Simon, Markus Stadler, Othmar Staffelbach, Doug R. Stinson, S. Trigila, Ugo Vaccaro, Serge Vaudenay, Jeroen van de Graaf, P. R. Wild, William Wolfowicz. The Program Committee appreciates their effort.

The rump session was chaired by Yvo Desmedt. There were 23 presentations, of which 11 appear in the proceedings.

Special thanks to Carlo Blundo and Giovanni Di Crescenzo for their help. Finally, I would like to thank everyone who submitted to Eurocrypt '94.

University of Salerno, Italy  
July 1995

Alfredo De Santis  
Program Chair, EUROCRYPT '94

# EUROCRYPT '94

took place in Perugia, Italy  
May 9–12, 1994

Sponsored by the  
*International Association for Cryptologic Research*

## General Chair

William Wolfowitz, Fondazione Ugo Bordoni, Rome, Italy

## Program Chair

Alfredo De Santis, Università di Salerno, Italy

## Program Committee

Ernie Brickell	Sandia Labs, USA
Claude Crepeau	CNRS, France
Yvo Desmedt	Univ. of Wisconsin, USA
Adina Di Porto	Fondazione Bordoni, Italy
Dieter Gollman	Univ. of London, UK
Louis Guillou	CCETT, France
Ueli Maurer	ETH Zurich, Switzerland
David Naccache	Gemplus, France
Tatsuaki Okamoto	NTT Labs, Japan
Jacques Stern	ENS-DMI, France
Moti Yung	IBM T. J. Watson Research Center, USA

# Contents

## Secret Sharing

Visual cryptography . . . . .	1
<i>Moni Naor and Adi Shamir</i>	
The size of a share must be large . . . . .	13
<i>L. Csirmaz</i>	
A linear construction of perfect secret sharing schemes . . . . .	23
<i>M. van Dijk</i>	
On the dealer's randomness required in secret sharing schemes . . . . .	35
<i>C. Blundo, A. Giorgio Gaggia and D. R. Stinson</i>	

## Hash functions

Black box cryptanalysis of hash networks based on multipermutations . .	47
<i>C. P. Schnorr and S. Vaudenay</i>	
A practical attack against knapsack based hash functions . . . . .	58
<i>A. Joux and L. Granboulan</i>	

## Signatures I

The blinding of weak signatures . . . . .	67
<i>M. Franklin and M. Yung</i>	
Can D.S.A. be improved? Complexity trade-offs with the digital signature standard . . . . .	77
<i>D. Naccache, D. M'Raihi, S. Vaudenay and D. Rphaeli</i>	
Designated confirmer signatures . . . . .	86
<i>D. Chaum</i>	

## Cryptosystems

Optimal asymmetric encryption . . . . .	92
<i>M. Bellare and P. Rogaway</i>	
A multiple-iterated trapdoor for dense compact knapsacks . . . . .	112
<i>G. Orton</i>	
On the security of some cryptosystems based on error-correcting codes . .	131
<i>F. Chabaud</i>	

## Zero-Knowledge and Protocol Methodology

Parallel divertibility of proofs of knowledge . . . . .	140
<i>L. Chen, I.B. Damgård and T.P. Pedersen</i>	
Methodology for digital money based on general cryptographic tools . . .	156
<i>S. D'Amiano and G. Di Crescenzo</i>	

## Signatures II

New group signature schemes . . . . .	171
<i>L. Chen and T.P. Pedersen</i>	
Message recovery for signature schemes based on the discrete logarithm problem . . . . .	182
<i>K. Nyberg and R. A. Rueppel</i>	
Threshold-multisignature schemes where suspected forgery implies traceability of adversarial shareholders . . . . .	194
<i>C.-M. Li, T. Hwang and N.-Y. Lee</i>	

## Pseudorandom Generators

The self-shrinking generator . . . . .	205
<i>W. Meier and O. Staffelbach</i>	
Feedback registers based on ramified extensions of the 2-adic numbers . .	215
<i>M. Goresky and A. Klapper</i>	



A general lower bound for the linear complexity of the product of shift-register sequences . . . . .	223
<i>R. Göttert and H. Niederreiter</i>	
Embedding and probabilistic correlation attacks on clock-controlled shift registers . . . . .	230
<i>J. Dj. Golić and L. O'Connor</i>	

## Authentication Codes

Near optimal unconditionally secure authentication . . . . .	244
<i>R. Taylor</i>	
Authentication codes in plaintext and chosen-content attacks . . . . .	254
<i>R. Safavi-Naini and L. Tombak</i>	

## Key Agreement and Key Distribution

Linking information reconciliation and privacy amplification . . . . .	266
<i>C. Cachin and U. M. Maurer</i>	
A secure and efficient conference key distribution system . . . . .	275
<i>M. Burmester and Y. Desmedt</i>	
Space requirements for broadcast encryption . . . . .	287
<i>C. Blundo and A. Cresti</i>	
How to break and repair Leighton and Micali's key agreement protocol . .	299
<i>Y. Zheng</i>	

## Protocols

Single-term divisible electronic coins . . . . .	306
<i>T. Eng and T. Okamoto</i>	
Formal requirements for key distribution protocols . . . . .	320
<i>P. Syverson and C. Meadows</i>	
Breaking an efficient anonymous channel . . . . .	332
<i>B. Pfitzmann</i>	

## Cryptanalysis and Block Ciphers

On Matsui's linear cryptanalysis . . . . .	341
<i>E. Biham</i>	
Links between differential and linear cryptanalysis . . . . .	356
<i>F. Chabaud and S. Vaudenay</i>	
On correlation between the order of S-boxes and the strength of DES . .	366
<i>M. Matsui</i>	
Relationships among nonlinearity criteria . . . . .	376
<i>J. Seberry, X.-M. Zhang and Y. Zheng</i>	

## Number Theory and Algorithms

Efficient exponentiation using precomputation and vector addition chains	389
<i>P. de Rooij</i>	
MIMD-factorisation on hypercubes . . . . .	400
<i>F. Damm, F.-P. Heider and G. Wambach</i>	

## Rump Session

New attacks on all double block length hash functions of hash rate 1, including the parallel-DM . . . . .	410
<i>L. R. Knudsen and X. Lai</i>	
New potentially 'weak' keys for DES and LOKI . . . . .	419
<i>L. R. Knudsen</i>	
Blackmailing using undeniable signatures . . . . .	425
<i>M. Jakobsson</i>	
Blind signatures based on the discrete logarithm problem . . . . .	428
<i>J. L. Camenisch, J.-M. Piveteau and M. A. Stadler</i>	
Comments on soviet encryption algorithm . . . . .	433
<i>C. Charnes, L. O'Connor, J. Pieprzyk, R. Safavi-Naini and Y. Zheng</i>	
Linear approximation of block ciphers . . . . .	439
<i>K. Nyberg</i>	

Memory efficient variants of public-key schemes for smart card applications . . . . .	445
<i>A. Shamir</i>	
A systematic attack on clock controlled cascades . . . . .	450
<i>R. Menicocci</i>	
On $A^2$ -codes including arbiter's attacks . . . . .	456
<i>T. Johansson and B. Smeets</i>	
An improvement of Davies' attack on DES . . . . .	461
<i>E. Biham and A. Biryukov</i>	
Q-deformed quantum cryptography . . . . .	468
<i>J. Hruby</i>	
 Author Index . . . . .	 473