

# Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

547

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



D. W. Davies (Ed.)

# Advances in Cryptology— EUROCRYPT '91

Workshop on the Theory and Application  
of Cryptographic Techniques  
Brighton, UK, April 8-11, 1991  
Proceedings

**Springer-Verlag**

Berlin Heidelberg New York

London Paris Tokyo

Hong Kong Barcelona

Budapest

Series Editors

Gerhard Goos  
GMD Forschungsstelle  
Universität Karlsruhe  
Vincenz-Priessnitz-Straße 1  
W-7500 Karlsruhe, FRG

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

Volume Editor

Donald W. Davies  
Royal Holloway and Bedford New College, Univ. of London  
Egham Hill, Surrey TW 20 0EX, UK

CR Subject Classification (1991): E.3-4, D.4.6, H.2.0, G.2.1

ISBN 3-540-54620-0 Springer-Verlag Berlin Heidelberg New York  
ISBN 0-387-54620-0 Springer-Verlag New York Berlin Heidelberg

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 1991  
Printed in Germany

Typesetting: Camera ready by author  
Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.  
45/3140-543210 - Printed on acid-free paper

# Preface

A series of open workshops devoted to modern cryptology began in Santa Barbara, California in 1981 and was followed in 1982 by a European counterpart in Burg Feurstein, Germany. The series has been maintained with summer meetings in Santa Barbara and spring meetings somewhere in Europe. At the 1983 meeting in Santa Barbara the International Association for Cryptologic Research was launched and it now sponsors all the meetings of the series.

Following the tradition of the series, papers were invited in the form of extended abstracts and were reviewed by the programme committee, which selected those to be presented. After the meeting, full papers were produced, in some cases with improvements and corrections. These papers form the main part of the present volume. They are placed in the same order that they took at the meeting and under the same headings, for ease of reference by those who attended. The classification under these headings was a little arbitrary, needing to fit the timing of the day's activities, but it makes a workable method of arrangement.

Also following tradition, a "rump session" was held during one evening, under the effective chairmanship of John Gordon. These were short presentations and those present found them to have some real interest, therefore we have taken the unusual step of including short papers contributed by the rump session speakers at the end of this volume, with a necessarily simplified review process.

There was no attempt by the programme committee to guide the programme towards particular themes, though the interests of the committee members may have influenced the shape of the meeting. In our admittedly rough classification the biggest group was about sequences, the term interpreted rather widely. The next biggest group concerned cryptanalysis, which was welcomed because cryptanalysis is the criterion by which algorithms and protocols in cryptography must be judged.

Zero-knowledge interactive protocols figured less this year than at earlier meetings - a consequence of the submissions we received, not of policy.

Smaller groups of papers dealt with S-box criteria, signatures and new ideas in public key cryptography. Then there were many papers placed into sessions labelled "theory" and "applications".

My task as programme chair was made easier by the high quality of papers we received, though we regretted having to reject some of the papers because of time limitations. I would like to thank the programme committee for its hard work of reviewing papers and the organizing committee for ensuring that everything ran smoothly, including the social events. Then, of course, the authors deserve many thanks for favouring Eurocrypt '91 with the publication of their excellent work and for preparing their final papers with (in most cases) admirable despatch.

London, August 1991

Donald W. Davies

# EUROCRYPT '91

**General Chairman:**

Andrew J. Clark

(Logica Aerospace and Defence Ltd.)

**Organizing Committee:**

Keith Martin

(Royal Holloway and Bedford New College, Univ. of London)

Martin Meikle-Small (Aspen Consultants)

Ben Meisner (RHBNC)

Kathleen Quinn (RHBNC)

Matthew Robshaw (RHBNC)

**Program Chairman:**

Donald W. Davies (RBHNC)

**Program Committee:**

Thomas Beth (Univ. of Karlsruhe)

Colin Boyd (Univ. of Manchester)

Norbert Cot (EHEI Université, Paris)

Viveke Fåk (Linköping University)

John Gordon (Cybermation Limited)

Siegfried Herda (GMD, Germany)

Arjen Lenstra (Bellcore, NJ)

Tsutomu Matsumoto (Yokohama National Univ.)

Fred Piper (RHBNC)

Claus Schnorr (Universität Frankfurt)

**EUROCRYPT '91 was sponsored by:**

International Association for Cryptologic Research (IACR)

in association with:

Logica Aerospace and Defence Limited

ABN Bank

Coopers and Lybrand Deloitte

Northern Telecom

with additional support from:

Computer Security Limited

IBM United Kingdom Limited



# Contents

## Cryptanalysis I

Differential Cryptanalysis of Feal and N-Hash E. Biham, A. Shamir . . . . .	1
Markov Ciphers and Differential Cryptanalysis X. Lai, J.L.Massey, S. Murphy. . . . .	17
The Knapsack Hash Function Proposed at Crypto '89 Can be Broken P. Camion, J. Patarin . . . . .	39

## Cryptanalysis II

An Improved Low-Density Subset Sum Algorithm M.J. Coster, B.A. LaMacchia, A.M. Odlyzko, C.P. Schnorr . . . . .	54
Cryptanalysis of McEliece's Public-Key Cryptosystem V.I. Korzhik, A.I. Turkin . . . . .	68
On the Security of the Schnorr Scheme Using Preprocessing P. de Rooij . . . . .	71

## Zero Knowledge and Oblivious Transfer

Broadcast Interactive Proofs M. Burmester, Y. Desmedt . . . . .	81
Direct Zero Knowledge Proofs of Computational Power in Five Rounds T. Okamoto, D. Chaum, K. Ohta . . . . .	96
On the Reversibility of Oblivious Transfer C. Crépeau, M. Sántha . . . . .	106

## Sequences I

Ziv-Lempel Complexity for Periodic Sequences and its Cryptographic Application S. Mund . . . . .	114
A Secret Key Cryptosystem by Iterating a Chaotic Map T. Habutsu, Y. Nishio, I. Sasase, S. Mori . . . . .	127
Boolean Functions Satisfying Higher Order Propagation Criteria B. Preneel, R. Govaerts, J. Vandewalle . . . . .	141

## Sequences II

The Maximum Order Complexity of Sequence Ensembles C.J.A. Jansen . . . . .	153
The Number of Output Sequences of a Binary Sequence Generator J.D. Golic . . . . .	160
Linear Complexity of Periodically Repeated Random Sequences Z.D. Dai, J.H. Yang . . . . .	168

## Sequences III

On a Fast Correlation Attack on Certain Stream Ciphers V. Chepyzhov, B. Smeets . . . . .	176
Analysis of Pseudo Random Sequences Generated by Cellular Automata W. Meier, O. Staffelbach . . . . .	186
On Binary Sequences from Recursions “modulo $2^e$ ” Made Non-Linear by the Bit-by-Bit “XOR” Function W.G. Chambers, Z.D. Dai . . . . .	200

## Signatures

Weaknesses of Undeniable Signature Schemes Y. Desmedt, M. Yung . . . . .	205
Distributed Provers with Applications to Undeniable Signatures T. P. Pedersen . . . . .	221
Interactive Bi-Proof Systems and Undeniable Signature Schemes A. Fujioka, T. Okamoto, K. Ohta . . . . .	243
Group Signatures D. Chaum, E. van Heyst . . . . .	257

## Theory I

Enhancing Secrecy by Data Compression: Theoretical and Practical Aspects C. Boyd . . . . .	266
Factoring Integers and Computing Discrete Logarithms via Diophantine Approximation C.P. Schnorr . . . . .	281
Some Considerations Concerning the Selection of RSA Moduli K. Huber . . . . .	294
On the Use of Interconnection Networks in Cryptography M. Portz . . . . .	302



**Theory II**

Non Supersingular Elliptic Curves for Public Key Cryptosystems  
 T. Beth, F. Schaefer . . . . . 316

Building Cyclic Elliptic Curves Modulo Large Primes  
 F. Morain . . . . . 328

On the Complexity of Hyperelliptic Discrete Logarithm Problem  
 H. Shizuya, T. Itoh, K. Sakurai. . . . . 337

**S-Box Criteria**

An Expanded Set of S-Box Design Criteria Based on Information Theory  
 and its Relation to Differential-Like Attacks  
 M.H. Dawson, S.E. Tavares . . . . . 352

Enumerating Nondegenerate Permutations  
 L. O'Connor . . . . . 368

Perfect Nonlinear S-Boxes  
 K. Nyberg . . . . . 378

**Applications I**

A Formal Approach to Security Architectures  
 R.A. Rueppel . . . . . 387

Discrete Logarithm Based Protocols  
 P. Horster, H.-J. Knobloch . . . . . 399

Human Identification Through Insecure Channel  
 T. Matsumoto, H. Imai . . . . . 409

The Automated Cryptanalysis of Analog Speech Scramblers  
 B. Goldberg, E. Dawson, S. Sridharan . . . . . 422

**Applications II**

A Construction for One Way Hash Functions and Pseudorandom Bit Generators  
 B. Sadeghiyan, J. Pieprzyk . . . . . 431

ESIGN: An Efficient Digital Signature Implementation for Smart Cards  
 A. Fujioka, T. Okamoto, S. Miyaguchi . . . . . 446

New Approaches to the Design of Self-Synchronizing Stream Ciphers  
 U.M. Maurer . . . . . 458

Randomized Authentication Systems  
 J. Pieprzyk, R. Safavi-Naini . . . . . 472

## Public Key Cryptography

Ideals over a Non-Commutative Ring and Their Application in Cryptology  
E.M. Gabidulin, A.V. Paramonov, O.V. Tretjakov . . . . . 482

Self-Certified Public Keys  
M. Girault . . . . . 490

Non-Interactive Public-Key Cryptography  
U.M. Maurer, Y. Yacobi . . . . . 498

## Short Papers presented at the “Rump Session”

Hash Functions and Graphs with Large Girths  
G. Zémor . . . . . 508

Dickson Pseudoprimes and Primality Testing  
W.B. Müller, A. Oswald . . . . . 512

Equivalent Goppa Codes and Trapdoors to McEliece's Public Key Cryptosystem  
J.K. Gibson . . . . . 517

A Threshold Cryptosystem Without a Trusted Party  
T.P. Pedersen . . . . . 522

A Comparison of Cryptanalytic Principles Based on Iterative Error-Correction  
M.J. Mihaljevic, J.D. Golic . . . . . 527

Cryptanalysis of the Chaotic-Map Cryptosystem Suggested at EUROCRYPT '91  
E. Biham . . . . . 532

How to Broadcast a Secret  
S. Berkovits . . . . . 535

Probabilistic Analysis of Elementary Randomizers  
J. Pieprzyk . . . . . 542

Race Integrity Primitives Evaluation (RIPE): A Status Report  
B. Preneel, D. Chaum, W. Fumy, C.J.A. Jansen, P. Landrock, G. Roelofsen . . . . . 547

The Information Leakage Through a Randomly Generated Function  
L. Brynielsson . . . . . 552

Some Weaknesses of “Weaknesses of Undeniable Signatures”  
D. Chaum . . . . . 554