Lecture Notes in Computer Science 658
Edited by G. Goos and J. Hartmanis

R. A. Rueppel (Ed.)

Advances in Cryptology – EUROCRYPT '92

Workshop on the Theory and Application
of Cryptographic Techniques
Balatonfüred, Hungary, May 24-28, 1992
Proceedings

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Volume Editor

Rainer A. Rueppel
R3 Security Engineering
Bahnhofstr. 242, CH-8623 Wetzikon, Switzerland

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

ISBN 3-540-56413-6 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-56413-6 Springer-Verlag New York Berlin Heidelberg

Typesetting: Camera ready by author
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 Feuerstein, 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.

Eurocrypt '92 in Hungary was a special meeting in many ways. For the first time, it was held in an Eastern European country. Our charming Hungarian hosts turned the conference into an unforgettable experience for all of us. Also for the first time, the General Chair and the Program Chair were based in different countries. The Program Committee was selected very internationally, which implied that joint meetings were impossible in the course of setting the program. It was encouraging to see how swiftly disputes could be resolved by electronic mail. To ease its burden, the official Program Committee of Eurocrypt '92 obtained help from many renowned researchers and scientists. Here is the final list of all those people (that I know of) who helped during the refereeing phase.

> Brandt, Brickell, Charpin, Crépeau, Csirmaz, Damgård, Denes, Desmedt, Feigenbaum, Fell, Fujioka, Girault, Golic, Helleseth, Itoh, Joux, Kenyon, Koyama, Kurosawa, Landrock, Matsui, Matsumoto, McCurley, Merritt, Miyaguchi, Miyaji, Morain, Morita, Nemetz, Odlyzko, Ohta, Okamoto, Quisquater, Rueppel, Sako, Sakurai, Santha, Seberry, Shamir, Simmons, Staffelbach, Stern, Tanaka, Vajda, Valle, Yang, Yung.

The Rump Session, this time held more in the spirit of a recent results session, was chaired by Laszlo Csirmaz. Some of the presentations, after a simplified review procedure, were selected for publication in these proceedings. They can be found at the end of this volume.

For the first time, a panel discussion was organized, entitled "The Eurocrypt '92 Controversial Issue: Trapdoor Primes and Moduli". The topic was mainly motivated by the public debate on the draft standard on digital signatures proposed by NIST. The panel members produced an interesting report which is included in this volume.

Following the tradition of the series, the authors produced full papers after the meeting, in some cases with revisions. 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.

My thanks go to the "extended" Program Committee, to the General Chair Tibor Nemetz, to the Organizing Committee, and last but not least to the authors who contributed their recent results. They all have invested their time and effort to make Eurocrypt '92 a success.

Zurich, October 1992 Rainer A. Rueppel

Contents

Secret Sharing

Graph decompositions and secret sharing schemes
C. Blundo, A. De Santis, D.R. Stinson, U. Vaccaro 1

Classification of ideal homomorphic threshold schemes over finite Abelian groups
Y. Frankel, Y. Desmedt 25

Hash Functions

FFT hashing is not collision-free
T. Baritaud, H. Gilbert, M. Girault 35

FFT-hash II, efficient cryptographic hashing
C.P. Schnorr 45

Hash functions based on block ciphers
X. Lai, J.L. Massey 55

Differential cryptanalysis mod 2^32 with applications to MD5
T.A. Berson 71

Block Ciphers

A new method for known plaintext attack of FEAL cipher
M. Matsui, A. Yamagishi 81

On the construction of highly nonlinear permutations
K. Nyberg 92

The one-round functions of the DES generate the alternating group
R. Wernsdorf 99

Stream Ciphers

Correlation via linear sequential circuit approximation of combiners with memory
J.D. Golić 113

Convergence of a Bayesian iterative error-correction procedure on a noisy shift register sequence
M.J. Mihaljević, J.D. Golić 124

Suffix trees and string complexity
L. O'Connor, T. Snider 138

Public Key I

Attacks on protocols for server-aided RSA computation
B. Pfitzmann, M. Waidner 153

Public-key cryptosystems with very small key lengths
G. Harper, A. Menezes, S. Vanstone 163

Resource requirements for the application of addition chains in modulo exponentiation
J. Sauerbrey, A. Dietel 174

Factoring

Massively parallel elliptic curve factoring
B. Dixon, A.K. Lenstra 183

The Eurocrypt '92 Controversial Issue

Trapdoor Primes and Moduli

Panel Report 194

Public Key II

Fast exponentiation with precomputation
E.F. Brickell, D.M. Gordon, K.S. McCurley, D.B. Wilson 200

Batch Diffie-Hellman key agreement systems and their application to portable communications
M.J. Beller, Y. Yacobi 208

High-speed implementation methods for RSA scheme
K. Iwamura, T. Matsumoto, H. Imai 221

Pseudo-random Permutation Generators

A simplified and generalized treatment of Luby-Rackoff pseudorandom permutation generators
U.M. Maurer 239

How to construct pseudorandom and super pseudorandom permutations from one single pseudorandom function
J. Patarin 256

A construction for super pseudorandom permutations from a single pseudorandom function
B. Sadeghiyan, J. Pieprzyk 267

Complexity Theory and Cryptography I

How to break a "secure" oblivious transfer protocol
D. Beaver 285

Uniform results in polynomial-time security
P. Barbaroux 297

Cryptographic protocols provably secure against dynamic adversaries
D. Beaver, S. Haber 307

Zero-Knowledge

Secure bit commitment function against divertibility
K. Ohta, T. Okamoto, A. Fujioka 324

Non-interactive circuit based proofs and non-interactive perfect zero-knowledge with preprocessing
I. Damgård 341

Tools for proving zero knowledge
I. Biehl, J. Buchmann, B. Meyer, C. Thiel, C. Thiel 356

Digital Signatures and Electronic Cash

How to make efficient fail-stop signatures
E. van Heyst, T.P. Pedersen 366

Which new RSA signatures can be computed from RSA signatures, obtained in a specific interactive protocol?
J.-H. Evertse, E. van Heyst 378

Transferred cash grows in size
D. Chaum, T.P. Pedersen 390

Complexity Theory and Cryptography II

Local randomness in candidate one-way functions
H. Niederreiter, C.P. Schnorr 408

How intractable is the discrete logarithm for a general finite group
T. Okamoto, K. Sakurai, H. Shizuya 420

Factoring with an Oracle
U.M. Maurer 429

Applications

Secure audio teleconferencing: a practical solution
R. Heiman 437

Selected Papers from the Rump Session

Secure conference key distribution schemes for conspiracy attacks
K. Koyama 449

A note on discrete logarithms with special structure
R. Heiman 454

A remark on a non-interactive public-key distribution system
U.M. Maurer, Y. Yacobi 458

Security bounds for parallel versions of identification protocols
L. Chen, Y. Damgård 461

Information-theoretic bounds for authentication frauds
A. Sgarro 467

A generalized correlation attack with a probabilistic constrained edit distance
J.D. Golić, S.V. Petrović 472

Systolic arrays for modular exponentiation using Montgomery method
K. Iwamura, T. Matsumoto, H. Imai 477

On the development of a fast elliptic curve cryptosystem
G.B. Agnew, R.C. Mullin, S.A. Vanstone 482

A Montgomery-suitable Fiat-Shamir-like authentication scheme
D. Naccache 488

Author Index 493