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

Volume Editor

Alfredo De Santis
Dipartimento di Informatica edApplicazioni, 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

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 Wolfowitcz 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 Of these, 2 were withdrawn and 36 were selected for presentation and publication in the proceedings.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 Filipponi, 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 Wolfowitcz, 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

Hash functions

Signatures I

Cryptosystems

Zero-Knowledge and Protocol Methodology

Signatures II

Pseudorandom Generators

Authentication Codes

Key Agreement and Key Distribution

Protocols

Cryptanalysis and Block Ciphers

Number Theory and Algorithms

Rump Session