Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

304

David Chaum Wyn L. Price (Eds.)

Advances in Cryptology – EUROCRYPT '87

Workshop on the Theory and Application
of Cryptographic Techniques
Amsterdam, The Netherlands, April 13–15, 1987
Proceedings

Springer-Verlag
Berlin Heidelberg New York London Paris Tokyo

Editorial Board

D. Barstow W. Brauer P. Brinch Hansen D. Gries D. Luckham
C. Moler A. Pnueli G. Seegmüller J. Stoer N. Wirth

Editors

David Chaum
Centre for Mathematics and Computer Science (CWI)
Kruislaan 413, 1098 SJ Amsterdam, The Netherlands

Wyn L. Price
National Physical Laboratory
Teddington, Middlesex TW11 OLW, U.K.

Workshop Organizers:

General Chairman:	D. Chaum (CWI)	
Programme Committee:	W.L. Price (NPL), Chairman	T. Herlestam (U. Lund)
	T. Beth (U. Karlsruhe)	F. Piper (U. London)
	J.-H. Evertse (CWI)	J.J. Quisquater (Philips)
	L. Guillou (CCETT)	
Organising Committee:	J. van de Graaf (CWI)	G. Roelofsen (PTT-DNL)
	C.J. Jansen (Philips USFA)	J. van Tilburg (PTT-DNL)

The workshop was sponsored by the
International Association for Cryptologic Research
with support from the
Centre for Mathematics and Computer Science (CWI), Amsterdam

CR Subject Classification (1987): D.4.6, E.3, F.1.3, F.2.1, H.2.0, H.2.4

ISBN 3-540-19102-X Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-19102-X Springer-Verlag New York Berlin Heidelberg

Library of Congress Cataloging-in-Publication Data. EUROCRYPT '87 (1987: Amsterdam, Netherlands) Advances in cryptology–EUROCRYPT '87. (Lecture notes in computer science; 304) Sponsored by the International Association for Cryptologic Research. Includes indexes. 1. Computers–Access control–Congresses. 2. Cryptography–Congresses. I. Chaum, David. II. Price, Wyn L., 1930-. III. International Association for Cryptologic Research. IV. Title. V. Series.
QA76.9.A25E963 1987 005.8 88-6664
ISBN 0-387-19102-X (U.S.)

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 other ways, and storage in data banks. Duplication of this publication or parts thereof is only permitted under the provisions of the German Copyright Law of September 9, 1965, in its version of June 24, 1985, and a copyright fee must always be paid. Violations fall under the prosecution act of the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1988

Printed in Germany

Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
2145/3140-543210

Preface

1987 marked a major upswing in attendance and contributions for this fifth in the series of Eurocrypt meetings. Response was so great that, to our regret, we were only able to accommodate less than half the submitted papers. Attendance was also up by a healthy margin.

The first two open meetings devoted to modern cryptography were organised independently: one by Allen Gersho during late Summer 1981 in Santa Barbara,[1] and the other by Thomas Beth and Rudiger Dierstein in Germany the following Spring.[2] David Chaum organised a successor to the Santa Barbara meeting the next year,[3] which launched the International Association for Cryptologic Research. The sponsorship of the association has enabled the series of annual Summer CRYPTO meetings in the U.S.[4-7] and annual Spring EUROCRYPT meetings in Europe to be continued unbroken.[8-11]

It is our pleasure to thank all those who contributed to making these proceedings possible: the authors, programme committee, organising committee, IACR officers and directors, and all the attendees.

We were all deeply saddened when we learned that Tore Herlestam, a member of the programme committee, had died unexpectedly. This volume is dedicated to him.

Amsterdam, the Netherlands D.C.
London, England W.L.P.
January 1988

[1] Advances in Cryptology: A Report on CRYPTO 81, Allen Gersho, Ed., UCSB ECE Report no. 82-04, Department of Electrical and Computer Engineering, Santa Barbara CA 93106.

[2] Cryptography: Proceedings, Burg Feuerstein 1982 (Lecture Notes in Computer Science; 149), Thomas Beth, Ed., Springer-Verlag, 1983.

[3] Advances in Cryptology: Proceedings of CRYPTO 82, David Chaum, Ronald L. Rivest, and Alan T. Sherman, Eds., Plenum NY, 1983.

[4] Advances in Cryptology: Proceedings of CRYPTO 83, David Chaum, Ed., Plenum NY, 1984.

[5] Advances in Cryptology: Proceedings of CRYPTO 84 (Lecture Notes in Computer Science; 196), G.R. Blakley and David Chaum, Eds., Springer-Verlag, 1985.

[6] Advances in Cryptology: Proceedings of CRYPTO 85 (Lecture Notes in Computer Science; 218), Hugh C. Williams, Ed., Springer-Verlag, 1986.

[7] Advances in Cryptology: Proceedings of CRYPTO 86 (Lecture Notes in Computer Science; 263), A.M Odlyzko, Ed., Springer-Verlag, 1987.

[8] No proceedings were published for EUROCRYPT 83, which was held in Udine Italy.

[9] Advances in Cryptology: Proceedings of EUROCRYPT 84 (Lecture Notes in Computer Science; 209), T. Beth, N. Cot, and I. Ingemarsson, Eds., Springer-Verlag, 1985.

[10] Advances in Cryptology: Proceedings of EUROCRYPT 85 (Lecture Notes in Computer Science; 219), Franz Pichler, Ed., Springer-Verlag, 1986.

[11] No proceedings were published for EUROCRYPT 86, which was held in Linköping, Sweden.

CONTENTS

SECTION I: SEQUENCES AND LINEAR COMPLEXITY

SECTION II: HARDWARE TOPICS

SECTION III: PUBLIC KEY TOPICS

SECTION IV: AUTHENTICATION AND SECURE TRANSACTIONS

SECTION V: HASH FUNCTIONS AND SIGNATURES

SECTION VI: SYMMETRIC CIPHERS: THEORY

SECTION VII: SYMMETRIC CIPHERS: APPLICATION