Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

453

J. Seberry J. Pieprzyk (Eds.)

Advances in Cryptology – AUSCRYPT '90

International Conference on Cryptology Sydney, Australia, January 8–11, 1990 Proceedings



Springer-Verlag

Berlin Heidelberg New York London Paris Tokyo Hong Kong Barcelona

Editorial Board

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

Editors

Jennifer Seberry Josef Pieprzyk Department of Computer Science, University College The University of New South Wales Austrialian Defence Force Academy Canberra, ACT 2600, Australia



CR Subject Classification (1987): E.3

ISBN 3-540-53000-2 Springer-Verlag Berlin Heidelberg New York ISBN 0-387-53000-2 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 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 Bersin Heidelberg 1990 Printed in Germany

Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr. 2145/3140-543210 – Printed on acid-free paper

AUSCRYPT'90

A Workshop on the Theory and Application of Cryptographic Techniques

January 8-11, 1990

The University of New South Wales, Sydney

Sponsored by

The International Association for Cryptologic Research in cooperation with

The IPACE Institute at UNSW

and

Department of Computer Science, University College, ADFA Centre for Communication Security Research

General Chair: Jennifer Seberry, The University of NSW, Canberra, Australia

Program Chairs: Josef Pieprzyk, The University of NSW, Canberra, Australia Rainer Rueppel, Crypto AG, Zug, Switzerland Scott Vanstone, University of Waterloo, Waterloo, Canada

Program Committee:

Gordon Agnew, University of Waterloo, Waterloo, Canada Ingemar Ingemarsson, University of Linkoping, Linkoping, Sweden Ron Mullin, University of Waterloo, Waterloo, Canada Wyn Price, National Physical Laboratory, Teddington, United Kingdom Rei Safavi-Naini, The University of NSW, Canberra, Australia

PREFACE

This book is the proceedings of AUSCRYPT '90, the first conference sponsored by the International Association for Cryptological Research to be held in the southern hemisphere and the first outside the EUROCRYPT series held in European countries each northern spring and the CRYPTO series held in Santa Barbara, USA each August.

The proceedings from these earlier conferences have been published in the Springer-Verlag Lecture Notes in Computer Science series since 1986.

Papers in this volume are organized into eleven sections. The first ten sections comprise all of the papers on the regular program, including a few papers on the program which, unfortunately, were not presented at the meeting. The last section contains some of the papers presented at the "Rump Session" organized by Josef Pieprzyk.

AUSCRYP'T '90 was attended by 95 people representing sixteen countries.

For the first time a skills workshop was held the day before the conference, with such eminent cryptographers as D. Gollmann (West Germany), I. Ingemarsson (Sweden), K. Ohta (Japan), R. Rueppel (Switzerland) and S. Vanstone (Canada) teaching in the area of their expertise. J. Seberry represented Australia at this event. Forty-one people attended the workshop.

It gives us great pleasure to express our thanks here to the members of the program committee: Dr R. Rueppel, Dr W.Price, and Dr I. Ingemarsson from Europe; Dr S. Vanstone, Dr R. Mullin, and Dr G. Agnew from North America; and Dr R. Safavi-Naini, and the other members of the Centre for Computer Security Research, for the rest of the world. They were all efficient, pleasant and wonderful co-workers.

Local organization was arranged by Ms C. Burke of the IPACE Institute, on the Sydney campus of The University of NSW. The conference dinner was held on a ferry on Sydney Harbour and was a spectacular success.

Many thanks to all the members of the Centre for Computer Security Research: Dr R. Safavi-Naini; Mr L. Brown; Ms L. Condie; Mr T. Hardjono; Mrs C. Newberry; Mr M. Newberry; Mr D. Rubie; Mrs E. Trott and Mrs E. Tait, all of whom readily worked at every task they were given to make the conference function smoothly and ensure its scientific success.

This conference was made possible by the support of the International Association for Cryptologic Research, The Centre for Computer Security Research, Prentice Hall Pty Ltd, and Telecom Australia.

> Jennifer Seberry Josef Pieprzyk

CONTENTS



SECTION 1: PUBLIC-KEY CRYPTOSYSTEMS

. . .

- ...

The implementation of elliptic curve cryptosystems Alfred Menezes, Scott A. Vanstone	2
	-
Kenji Koyama	14

SECTION 2: PSEUDORANDOMNESS AND SEQUENCES I

Continued fractions and Berlekamp-Massey algorithm Zongduo Dai, Kencheng Zeng	24
Nonlinear generators of binary sequences with controllable complexity and double key	
Gong Guang	32
K-M sequence is forwardly predictable	
Yang Yi Xian	37
Lower bounds on the weight complexities of cascaded binary sequences	
Cunsheng Ding	39

SECTION 3: NETWORK SECURITY

Secure user access control for public networks Pil Joong Lee	46
Formal specification and verification of secure communication protocols Svein J. Knapskog	58
Network security policy models Vijay Varadharajan	74
KEYMEX: an expert system for the design of key management	
schemes	
J. C. A. van der Lubbe, Dick E. Boekee	-96

SECTION 4: AUTHENTICATION

On the formal analysis of PKCS authentication protocols	
Klaus Gaarder, Einar Snekkenes	106
Some remarks on authentication systems	
Martin H. G. Anthony, Keith M. Martin, Jennifer Seberry,	
Peter Wild	122

Meet-in-the-mi	ddle attack on	digital signature s	chemes	
Kazuo Ohta, K	enji Koyama .			140

SECTION 5: PSEUDORANDOMNESS AND SEQUENCES II

A binary sequence generator based on Ziv-Lempel source coding Cees J. Jansen, Dick E. Boekee	6
A fast iterative algorithm for a shift register initial state reconstruction given the noisy output sequence Miodrag J. Mihaliević, Jovan D. Golić	5
Parallel generation of pseudo-random sequences Reihaneh Safavi-Naini	6
Large primes in stream cipher cryptography Kencheng Zeng, C. H. Yang, T. R. N. Rao	4

SECTION 6: BLOCK CIPHERS

Comparison of block ciphers Helen Gustafson, Ed Dawson, Bill Caelli
Key scheduling in DES type cryptosystems
Lawrence Brown, Jennifer Seberry
LOKI - a cryptographic primitive for authentication and secrecy applications
Lawrence Brown, Josef Pieprzyk, Jennifer Seberry
Permutation generators of alternating groups Josef Pieprzyk, Xian Mo Zhang, 237

SECTION 7: ZERO-KNOWLEDGE PROTOCOLS

Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms David Chaum	246
A (non-practical) three-pass identification protocol using coding theory	
Marc Girault	265
Demonstrating possession without revealing factors and its application Hiroki Shizuya, Kenji Koyama, Toshiya Itoh	273
Anonymous one-time signatures and flexible untraceable electronic cash Barry Hayes	294

SECTION 8: THEORY

Dyadic matrices and their potential significance in cryptography Yang Yi Xian
A note on strong Fibonacci pseudoprimes Rudolf Lidl, Winfried B. Müller
On the significance of the directed acyclic word graph in cryptology Cees J. Jansen, Dick E. Boekee
Solving equations in sequences Kencheng Zeng, Mingiang Huang

SECTION 9: APPLICATIONS

The practical application of state of the art security in real environments	
Ronald Ferreira	34
RSA as a benchmark for multiprocessor machines	
Rodney H. Cooper, Wayne Patterson	-56
Range equations and range matrices: a study in statistical database security	
V. S. Alagar	60
Record encryption in distributed databases	
Thomas Hardjono	66

SECTION 10: IMPLEMENTATIONS

VLS1 design for exponentiation in $GF(2^n)$ W. Geiselmann, D. Gollmann	98
A fast modular-multiplication module for smart cards Hikaru Morita	06
Minòs: extended user authentication Michael Newberry	10

SECTION 11: RUMP SESSION

Universal logic sequences Ed Dawson, Bruce Goldburg	,	•								426
The three faces of information security John M. Carroll			 							4 33
Secure cryptographic initialization Mark Ames										451