Lecture Notes in Computer Science 718

Edited by G. Goos and J. Hartmanis

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

Jennifer Seberry Yuliang Zheng (Eds.)

Advances in Cryptology – AUSCRYPT '92

Workshop on the Theory and Application
of Cryptographic Techniques
Gold Coast, Queensland, Australia
December 13-16, 1992
Proceedings

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

Series Editors

Gerhard Goos
Universität Karlsruhe
Postfach 69 80
Vincenz-Priessnitz-Straße 1
D-76131 Karlsruhe, Germany

Juris Hartmanis
Cornell University
Department of Computer Science
4130 Upson Hall
Ithaca, NY 14853, USA

Volume Editors

Jennifer Seberry
Yuliang Zheng
Department of Computer Science, University of Wollongong
Northfields Avenue, Wollongong NSW 2522, Australia

CR Subject Classification (1991): E.3-4, D.4.6, G.2.1, C.2.0, K.6.5

ISBN 3-540-57220-1 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-57220-1 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 1993
Printed in Germany

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

Preface

The AUSCRYPT'92 conference held on the Gold Coast, Queensland, Australia, 13-16 December, 1992 is the second conference held in the Southern Hemisphere in cooperation with the International Association for Cryptologic Research. The conference was very enjoyable and ran very smoothly, largely due to the efforts of the General Chair, Professor Bill Caelli of the Queensland University of Technology and his colleagues Ed Dawson, Barry Arnison, Helen Bergen, Eleanor Crosby, Diane Donovan, Ian Graham, Helen Gustafson, and Lauren Nielson. There were 114 attendees from 18 countries and 5 continents.

This is the third conference held outside the EUROCRYPT series, held in European countries each northern spring, and the CRYPTO series held in Santa Barbara, California, USA each August. The other two were AUSCRYPT'90 held in Sydney, New South Wales, Australia in January 1990 and ASIACRYPT'91 held in Fujiyoshida, Japan in December 1992.

There were 77 submissions from 18 countries and 55 were accepted from 15 countries. Thirty were submitted from Asia and 15 accepted, 17 from Europe and 13 accepted, 12 from North America and 8 accepted and 18 from Australia of which 9 were accepted. In addition there were 7 presentations representing 5 countries at the rump sessions. After refereeing, 3 of them were selected to be published in these proceedings. All refereeing was carried out blind: no names were attached to papers. Programme Committee members' submissions were anonymous and went through exactly the same refereeing procedure as all other papers except that they were always sent to referees not in their own country. In addition the Committee chose four invited speakers: Yvo Desmedt from University of Wisconsin-Milwaukee, USA, Peter Landrock, the IACR President from Denmark, Valery Korzhik from Russia and John Snare, Australia's representative on the International Standards Committees. Please remember that these invited talks were not refereed and the authors bear full responsibility for their contents.

It is our pleasure to acknowledge the efforts of all those who contributed to making the conference a success. We especially wish to thank the members of the Programme Committee: Mike Burmester (RHNBC, University of London, UK), Yvo Desmedt (University of Wisconsin-Milwaukee, USA), Hideki Imai (University of Tokyo but formerly of Yokohama National University, Japan), Svein Knapskog (University of Trondheim, Norway), Rudi Lidl (University of Tasmania, Hobart, Australia), John Loxton (Macquarie University, Sydney, Australia), Tsutomu Matsumoto (Yokohama National University, Japan), Josef Pieprzyk (University of Wollongong, New South Wales, Australia), Rei Safavi-Naini, (University of Wollongong, New South Wales, Australia) and the Programme Chair Jennifer Seberry (University of Wollongong, New South Wales, Australia). Many of these referees will have used other persons to advise and evaluate and we sincerely thank those anonymous persons. Josef Pieprzyk ably organized the Rump Session.

We must thank my two valuable helpers Tor Jomar Nordhagen (Norway) and Marc Gysin (Switzerland) who helped so much with the electronic processing, entering into the computer all referees' comments that came by snail mail, then helped to email and print letters for the acceptances and rejections so we could get comments to authors as speedily as possible.

We wish to thank all the authors for sending their submissions (even ones that were unsuccessful), the speakers, and all the participants of this and other IACR conferences. We have established a tradition for high quality research and we hope this continues.

Wollongong, New South Wales, Australia
July 1993

Jennifer Seberry
Yuliang Zheng

General Chair

Bill Caelli (Queensland University of Technology, Australia)

Program Chair

Jennifer Seberry (University of Wollongong, Australia)

Program Committee

Mike Burmester	(RHBNC, University of London, UK)
Yvo Desmedt	(University of Wisconsin-Milwaukee, USA)
Hideki Imai	(University of Tokyo, Japan)
Svein Knapskog	(University of Trondheim, Norway)
Rudi Lidl	(University of Tasmania, Australia)
John Loxton	(Macquarie University, Australia)
Tsutomu Matsumoto	(Yokohama National University, Japan)
Josef Pieprzyk	(University of Wollongong, Australia)
Rei Safavi-Naini	(University of Wollongong, Australia)

In cooperation with
The International Association for Cryptologic Research (IACR)
and
The Centre for Computer Security Research, University of Wollongong
and
The Information Security Research Centre, Queensland University of Technology

Table of Contents

Session 1: AUTHENTICATION AND SECRET SHARING I

Chair: Diane Donovan

Threshold cryptosystems (invited talk) 3
Y. Desmedt (University of Wisconsin-Milwaukee, USA)

Authentication codes with perfect protection 15
L. Tombak, R. Safavi-Naini (University of Wollongong, Australia)

Practical proven secure authentication with arbitration 27
Y. Desmedt (University of Wisconsin-Milwaukee, USA),
J. Seberry (University of Wollongong, Australia)

Session 2: AUTHENTICATION AND SECRET SHARING II

Chair: Josef Pieprzyk

Authentication codes under impersonation attack 35
R. Safavi-Naini, L. Tombak (University of Wollongong, Australia)

Cumulative arrays and geometric secret sharing schemes 48
W.-A. Jackson (RHBNC, University of London, UK),
K.M. Martin (University of Adelaide, Australia)

Nonperfect secret sharing schemes 56
W. Ogata, K. Kurosawa, S. Tsujii (Tokyo Institute of Technology, Japan)

A construction of practical secret sharing schemes using linear block codes . 67
M. Bertilsson, I. Ingemarsson (Linköping University, Sweden)

Session 3: SIGNATURES AND HASHING ALGORITHMS

Chair: Yvo Desmedt

HAVAL — a one-way hashing algorithm with variable length of output 83
Y. Zheng, J. Pieprzyk, J. Seberry (University of Wollongong, Australia)

On the power of memory in the design of collision resistant hash functions 105
B. Preneel, R. Govaerts, J. Vandewalle (Katholieke Universiteit Leuven, Belgium)

A practical digital multisignature scheme based on discrete logarithms 122
T. Hardjono (ATR Communications Research Laboratories, Japan),
Y. Zheng (University of Wollongong, Australia)

Group-oriented undeniable signature schemes
without the assistance of a mutually trusted party 133
L. Harn (University of Missouri-Kansas, USA),
S. Yang (University of Science and Technology of China, PRC)

Session 4: THEORY OF S-BOXES
Chair: Tsutomu Matsumoto

Highly nonlinear 0-1 balanced Boolean functions
satisfying strict avalanche criterion 145
J. Seberry, X.-M. Zhang (University of Wollongong, Australia)

Linear nonequivalence versus nonlinearity 156
C. Charnes, J. Pieprzyk (University of Wollongong, Australia)

Constructing large cryptographically strong S-boxes 165
J. Detombe, S.E. Tavares (Queen's University at Kingston, Canada)

Session 5: CRYPTANALYSIS
Chair: Peter Landrock

Nonasymptotic estimates of information protection efficiency
for the wire-tape channel concept (invited talk) 185
V. Korzhik, V. Yakovlev (Bronch-Bruevitch Technical Communications University, Russia)

Cryptanalysis of LOKI91 196
L.R. Knudsen (Aarhus University, Denmark)

Cryptanalysis of summation generator 209
E. Dawson (Queensland University of Technology, Australia)

Session 6: PROTOCOLS I
Chair: Rei Safavi-Naini

Secure addition sequence and its applications
on the server-aided secret computation protocols 219
C.-S. Laih, S.-M. Yen (National Cheng Kung University, Taiwan)

Subliminal channels for signature transfer and
their application to signature distribution schemes 231
K. Sakurai (Mitsubishi Electric Co., Japan),
T. Itoh (Tokyo Institute of Technology, Japan)

A practical secret voting scheme for large scale elections 244
A. Fujioka, T. Okamoto, K. Ohta (NTT Laboratories, Japan)

Privacy for multi-party protocols 252
T. Satoh, K. Kurosawa, S. Tsujii (Tokyo Institute of Technology, Japan)

Session 7: PROTOCOLS II
Chair: Ed Dawson

New protocols for electronic money 263
J.C. Pailles (SEPT, France)

Modelling and analyzing cryptographic protocols using Petri nets 275
B.B. Nieh, S.E. Tavares (Queen's University at Kingston, Canada)

On verifiable implicit asking protocols for RSA computation 296
T. Matsumoto (Yokohama National University, Japan),
H. Imai (University of Tokyo, Japan),
C.-S. Laih, S.-M. Yen (National Cheng Kung University, Taiwan)

Modified Maurer-Yacobi's scheme and its applications 308
C.H. Lim, P.J. Lee (Pohang Institute of Science and Technology, Korea)

Session 8: SEQUENCES
Chair: Rudi Lidl

The vulnerability of geometric sequences
based on fields of odd characteristic 327
A. Klapper (University of Manitoba, Canada)

A fast cryptographic checksum algorithm based on stream ciphers 339
X. Lai (Swiss Federal Institute of Technology, Switzerland),
R.A. Rueppel, J. Woollven (R^3 Security Engineering, Switzerland)

An approach to the initial state reconstruction of a clock-controlled
shift register based on a novel distance measure 349
M.J. Mihaljevic (University of Belgrade, Yugoslavia)

Construction of m-ary de Bruijn sequences 357
J.-H. Yang, Z.-D. Dai (Academia Sinica, PRC)

Session 9: PSEUDORANDOMNESS
Chair: Bill Caelli

Information technology security standards
— an Australian perspective (invited talk) 367
J. Snare (Telecom Research Laboratories, Australia)

Non-interactive generation of shared pseudorandom sequences 385
M. Cerecedo, T. Matsumoto (Yokohama National University, Japan),
H. Imai (University of Tokyo, Japan)

A generalized description of DES-based and
Benes-based permutation generators 397
M. Portz (RWTH Aachen, Germany)

Session 10: ODDS AND ENDS
Chair: Valery Korzhik

Prime generation with the Demytko-Miller-Trbovich algorithm 413
L. Condie (University of New England, Australia)

Construction of feebly-one-way families of permutations 422
A.P.L. Hiltgen (Swiss Federal Institute of Technology, Switzerland)

On bit correlations among preimages of
"many to one" one-way functions 435
K. Sakurai (Mitsubishi Electric Co., Japan),
T. Itoh (Tokyo Institute of Technology, Japan)

The fast cascade exponentiation algorithm and
its applications on cryptography 447
S.-M. Yen, C.-S. Laih (National Cheng Kung University, Taiwan)

Session 11: PUBLIC KEY CRYPTOGRAPHY I
Chair: Jennifer Seberry

The design of a conference key distribution system 459
C.-C. Chang (National Chung Cheng University, Taiwan),
T.-C. Wu (National Chiao Tung University, Taiwan),
C.-P. Chen (National Chung Cheng University, Taiwan)

Remarks on "The design of a conference key distribution system" 467
E. Zuk (Telecom Research Laboratories, Australia)

Public-key cryptosystem based on the discrete logarithm problem 469
L. Harn (University of Missouri-Kansas, USA),
S. Yang (University of Science and Technology of China, PRC)

Session 12: PUBLIC KEY CRYPTOGRAPHY II
Chair: John Snare

Elliptic curves over F_p suitable for cryptosystems 479
A. Miyaji (Matsushita Electric Industrial Co. LTD., Japan)

The probability distribution of the Diffie-Hellman key 492
C.P. Waldvogel, J.L. Massey (Swiss Federal Institute of Technology, Switzerland)

A modular exponentiation unit based on systolic arrays 505
J. Sauerbrey (Technische Universitat Munchen, Germany)

A comparison of key distribution patterns
constructed from circle geometries 517
C.M. O'Keefe (University of Adelaide, Australia)

Rump Session
Chair: Josef Pieprzyk

A block cipher method using combinations of different methods under the control of the user key 531
M. Rezny, E. Trimarchi (Queensland University of Technology, Australia)

An attack on two hash functions by Zheng-Matsumoto-Imai 535
B. Preneel, R. Govaerts, J. Vandewalle (Katholieke Universiteit Leuven, Belgium)

Primality testing with Lucas functions 539
R. Lidl (University of Tasmania, Australia),
W. B. Müller (Universität Klagenfurt, Austria)

Author Index 543