

Eiji Okamoto George Davida
Masahiro Mambo (Eds.)

Information Security

First International Workshop, ISW'97
Tatsunokuchi, Ishikawa, Japan
September 17-19, 1997
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Eiji Okamoto
School of Information Science
Japan Advanced Institute of Science and Technology
1-1 Asahidai Tatsunokuchi Nomi Ishikawa, 923-1292 Japan
E-mail: okamoto@jaist.ac.jp

George Davida
Department of Electrical Engineering and Computer Science
University of Wisconsin-Milwaukee
3200 N. Cramer Street, Milwaukee, WI 53201, USA
E-mail: davida@cs.uwm.edu

Masahiro Mambo
Education Center for Information Processing, Tohoku University
Kawauchi Aoba Sendai, 980-8576, Japan
E-mail: mambo@tohoku.ac.jp

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information security : first international workshop ; proceedings /
ISW '97, Tatsunokuchi, Ishikawa, Japan, September 17 - 19, 1997.
George Davida ... (ed.). - Berlin ; Heidelberg ; New York ; Barcelona
; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ;
Singapore ; Tokyo : Springer, 1998
(Lecture notes in computer science ; Vol. 1396)
ISBN 3-540-64382-6

CR Subject Classification (1991): E.3, G.2.1, D.4.6, K.6.5, F.2.1-2, C.2, J.1,
E.4

ISSN 0302-9743

ISBN 3-540-64382-6 Springer-Verlag Berlin Heidelberg New York

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 1998
Printed in Germany

Typesetting: Camera-ready by author
SPIN 10636992 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

ISW'97, the 1997 Information Security Workshop, was held at the Ishikawa High-Tech Conference Center in JAIST, Japan Advanced Institute of Science and Technology, Ishikawa, Japan, September 17-19. The workshop was sponsored by JAIST, Ministry of Education, Science, Sports and Culture, Engineering Sciences Society of IEICE (The Institute of Electronics, Information and Communication Engineers), Telecommunications Advancement Foundation, and Ishikawa Prefecture. The workshop was organized in cooperation with Tokyo Chapter of IEEE Information Theory, and Society of Information Theory and Its Applications. We are grateful to all these organizations for their support of the workshop.

One of the goals of ISW'97 was to give young researchers into the field of information security an opportunity to present papers at an international conference. For that purpose, a number of stipends were available to those unable to obtain funding to attend the workshop.

The workshop program addressed a range of topics from theory, technique, applications, and experimental work on topics relevant to information security and cryptography. The program committee invited Dr. Mihir Bellare (University of California at San Diego), Dr. Yvo Desmedt (University of Wisconsin at Milwaukee), Dr. Bart Preneel (Katholieke Universiteit Leuven, Belgium) and Dr. Yuliang Zheng (Monash University, Australia). Dr. George Robert Blakley (Texas A&M University) opened the workshop with general code theory and Dr. René Peralta (University of Wisconsin at Milwaukee) had a special talk on fast software encryption. Their talks were stimulating and informative.

The program committee accepted 25 papers from 39 submissions covering cryptanalysis, public-key cryptosystem, signature, hardware/software implementation, key management, key sharing, security management, electronic commerce and quantum cryptology. The accepted papers came from many countries: Australia, Belgium, Brazil, China, India, Korea, Singapore, Taiwan, USA, United Kingdom, and Japan. We commend the members of the program committee for this excellent program.

Organizing an international workshop is a time-consuming task. We would like to thank the steering committee members, organizing committee members, JAIST section for academic exchanges, and JAIST students in Dr. Okamoto's Laboratory for helping with many local details. We also thank all session chairs, speakers and authors who submitted papers and all participants at ISW'97.

February 1998

Eiji Okamoto
George Davida
Masahiro Mambo

Information Security Workshop (ISW'97)

Sponsored by

Japan Advanced Institute of Science and Technology
The Engineering Sciences Society of IEICE
The Ministry of Education, Science, Sports and Culture
The Telecommunications Advancement Foundation
Ishikawa Prefecture

In cooperation with

IEEE IT Society, Tokyo Chapter, and SITA

Steering Committee

Masayuki Kimura (**Co-chair**, JAIST, Japan)
Bob Blakley (**Co-chair**, Texas A&M, USA)
Masayasu Hata (Nagoya Inst. of Tech., Japan)
Hideki Imai (Univ. of Tokyo, Japan)
Yoshihiro Iwadare (Nagoya Univ., Japan)
Masao Kasahara (Kyoto Inst. of Tech., Japan)
Hatsukazu Tanaka (Kobe Univ., Japan)
Hideyoshi Tominaga (Waseda Univ., Japan)
Shigeo Tsujii (Chuo Univ., Japan)

Program Committee

George Davida (**Co-chair**, Univ. of Wisconsin, Milwaukee, USA)
Eiji Okamoto (**Co-chair**, JAIST, Japan)
Jinhui Chao (Chuo Univ., Japan)
Ivan Damgård (Århus Univ., Denmark)
Toru Fujiwara (Osaka Univ., Japan)
Akira Hayashi (Kanazawa Inst. of Tech., Japan)
Tzonelih Hwang (Cheng Kung Univ., Taiwan, R.O.C)
Toshiya Itoh (Tokyo Inst. of Tech., Japan)
Kunikatsu Kobayashi (Yamagata Univ., Japan)
Naohisa Komatsu (Waseda Univ., Japan)
Arjen Lenstra (Citibank, USA)
Tsutomu Matsumoto (Yokohama National Univ., Japan)
Shiho Moriai (TAO, Japan)
Yuko Murayama (Hiroshima City Univ., Japan)
Andrew Odlyzko (AT&T, USA)

René Peralta (Univ. of Wisconsin, Milwaukee, USA)
Philip Rogaway (Univ. of California, Davis, USA)
Ryuichi Sakai (Osaka Electro-Communication Univ., Japan)
Kouichi Sakurai (Kyushu Univ., Japan)
Hiroki Shizuya (Tohoku Univ., Japan)

Organizing Committee

Masahiro Mambo (**Chair**, Tohoku Univ., Japan)
Kunihiko Hiraishi (JAIST, Japan)
Mineo Kaneko (JAIST, Japan)
Yasushi Sengoku (Kanazawa Inst. of Tech., Japan)

Contents

Special Lecture

- A General Theory of Codes, II: Paradigms and Homomorphisms 1
G.R. Blakley and I. Borosh (Texas A&M Univ., USA)

Cryptanalysis

- Improving the Higher Order Differential Attack and Cryptanalysis of
the \mathcal{KN} Cipher 32
*Takeshi Shimoyama, Shiho Moriai (TAO, Japan) and
Toshinobu Kaneko (TAO and Science Univ. of Tokyo, Japan)*
- An Optimised Linear Attack on Pseudorandom Generators Using a
Non linear Combiner 43
*Hidema Tanaka, Tomoya Ohishi and
Toshinobu Kaneko (Science Univ. of Tokyo, Japan)*

Invited Lecture

- Cryptanalysis of Message Authentication Codes 55
Bart Preneel (Katholieke Univ. Leuven, Belgium)

Public-Key Cryptography

- The Least Witness of a Composite Number 66
R. Balasubramanian and S. V. Nagaraj (Inst. of Math. Sci., India)
- Fast Algorithm for Finding a Small Root of a Quadratic Modular
Equation 75
Hidenori Kuwakado and Hatsukazu Tanaka (Kobe Univ., Japan)
- Modified Finite Automata Public Key Cryptosystem 82
*Feng Bao, Robert H. Deng (Nat'l Univ. of Singapore, Singapore),
Xiang Gao (Millstar Elec. Pub. Group, USA) and
Yoshihide Igarashi (Gunma Univ., Japan)*
- Modified ElGamal Cryptosystem 96
*Daisuke Nakamura and Kunikatsu Kobayashi (Yamagata Univ.,
Japan)*
- Remarks on Blind Decryption 109
Kazuo Ohta (NTT Lab., Japan)

Special Lecture

- High-Speed Cryptography 116
George Davida and René Peralta (Univ. of Wisconsin-Milwaukee, USA)

Key Management

- Secure Applications of Low-Entropy Keys 121
John Kelsey, Bruce Schneier, Chris Hall (Counterpane Systems, USA) and David Wagner (U.C. Berkeley, USA)
- A Key Escrow System of the RSA Cryptosystem 135
Yoshiki Sameshima (Hitachi Software Eng., Japan)
- A Key Escrow System with Protecting User's Privacy by
 Blind Decoding 147
Kouichi Sakurai, Yoshinori Yamane, Shingo Miyazaki (Kyushu Univ., Japan) and Tohru Inoue (Adv. Mobile Telecomm. Sec. Tech. Research Lab., Japan)

Invited Lecture

- Some Recent Research Aspects of Threshold Cryptography 158
Yvo Desmedt (Univ. of Wisconsin-Milwaukee, USA)

Implementation(Hard/Soft)

- A High-Speed Small RSA Encryption LSI with
 Low Power Dissipation 174
A. Satoh, Y. Kobayashi, H. Nijima, N. Ooba, S. Munetoh and S. Sone (IBM Japan, Japan)
- The Case for a Secure Multi-Application Smart Card Operating
 System 188
Constantinos Markantonakis (Royal Holloway, Univ. of London, UK)
- An Augmented Family of Cryptographic Parity Circuits 198
Kenji Koyama (NTT C.S. Labs., Japan) and Routo Terada (Univ. of S. Paulo, Brazil)
- A New Byte-Oriented Block Cipher 209
Xun Yi, Kwok Yan Lam (Nat'l Univ. of Singapore, Singapore), Shi Xin Cheng and Xiao Hu You (Southeast Univ., P. R. China)

Invited Lecture

Practice-Oriented Provable-Security	221
<i>Mihir Bellare (Univ. of California at San Diego, USA)</i>	

Security Management

A Framework for the Management of Information Security	232
<i>Jussipekka Leiwo and Yuliang Zheng (Monash Univ., Australia)</i>	
Specifying Security in a Composite System	246
<i>J.-M. Kabasele-Tenday (Univ. catholique de Louvain, Belgium)</i>	
On Rough Sets and Inference Analysis	256
<i>Kan Zhang (Cambridge Univ., UK)</i>	

Signature/Authentication

Arbitrated Unconditionally Secure Authentication Scheme with Multi-senders	266
<i>Tzonelih Hwang and Chih-Hung Wang (Nat'l Cheng-Kung Univ., Taiwan, R.O.C.)</i>	
Group Signatures for Hierarchical Multigroups	273
<i>Seungjoo Kim (Sung-Kyun-Kwan Univ., Korea), Sangjoon Park (ETRI, Korea) and Dongho Won (Sung-Kyun-Kwan Univ., Korea)</i>	
Threshold Proxy Signature Schemes	282
<i>Kan Zhang (Cambridge Univ., UK)</i>	

Invited Lecture

Signcryption and Its Applications in Efficient Public Key Solutions	291
<i>Yuliang Zheng (Monash Univ., Australia)</i>	

Payment Scheme

A New Digital Cash Scheme Based on Blind Nyberg-Rueppel Digital Signature	313
<i>Khanh Quoc Nguyen, Yi Mu and Vijay Varadharajan (Univ. of Western Sydney, Australia)</i>	

An Incremental Payment Method for Internet Based Streaming Real-Time Media	321
<i>Andreas Fuchsberger (Royal Holloway, Univ. of London, UK)</i>	

Key Sharing

A New Identity-Based Key Exchange Protocol Minimizing Computation and Communication	328
<i>Shahrokh Saeednia (Univ. de Bruxelles, Belgium) and Rei Safavi-Naini (Univ. of Wollongong, Australia)</i>	
The Application of ID-Based Key Distribution Systems to an Elliptic Curve	335
<i>Hisao Sakazaki, Eiji Okamoto and Masahiro Mambo (JAIST, Japan)</i>	
On Reconciliation of Discrepant Sequences Shared through Quantum Mechanical Channels	345
<i>Kouichi Yamazaki, Masao Osaki and Osamu Hirota (Tamagawa Univ., Japan)</i>	

Author Index	357
---------------------------	------------