Lecture Notes in Computer Science 1787
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
*Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo*

JooSeok Song (Ed.)

Information Security and Cryptology – ICISC'99

Second International Conference
Seoul, Korea, December 9-10, 1999
Proceedings

Springer

Series Editors

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

Volume Editor

JooSeok Song
Yonsei University
Department of Computer Science
Seoul, Korea
E-mail: jssong@emerald.yonsei.acr.kr

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information security and cryptology : second international conference ; proceedings / ICISC '99, Seoul, Korea, December 9 - 10, 1999. JooSeok Song (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 2000
(Lecture notes in computer science ; Vol. 1787)
ISBN 3-540-67380-6

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

ISSN 0302-9743
ISBN 3-540-67380-6 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 is a company in the BertelsmannSpringer publishing group.
© Springer-Verlag Berlin Heidelberg 2000
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Christian Grosche
Printed on acid-free paper SPIN: 10719994 06/3142 5 4 3 2 1 0

Preface

The 2nd International Conference on Information Security and Cryptology (ICISC) was sponsored by the Korea Institute of Information Security and Cryptology (KIISC). It took place at Korea University, Seoul, Korea, December 9-10, 1999. Jong In Lee of Korea University was responsible for the organization.

The call for papers brought 61 papers from 10 countries on four continents. As in the last year the review process was totally blind. The information about authors or their affiliation was not given to Technical Program Committee (TPC) members. Each TPC member was random-coded and did not even know who was reviewing which paper. The 23 TPC members finally selected 20 top-quality papers for presentation at ICISC 1999 together with one invited talk. Serge Vaudenay gave an invited talk on “Provable Security for Conventional Cryptography”.

Many people contributed to ICISC’99. First of all I would like to thank all the authors who submitted papers. I am grateful to the TPC members for their hard work reviewing the papers and the Organization Committee members for all the supporting activities which made ICISC’99 a success. I would like to thank the Ministry of Information and Communication of Korea (MIC) which financially sponsored ICISC’99. Special thanks go to Pil Joong Lee and Heung Youl Youm who helped me during the whole process of preparation for the conference. Last, but not least, I thank my students, KyuMan Ko, Sungkyu Chie, and Chan Yoon Jung.

December 1999 Jooseok Song

ICISC'99

December 9-10, 1999, Korea University, Seoul, Korea

The 2nd International Conference on
Information Security and Cryptology

Sponsored by
Korea Institute of Information Security and Cryptology
(KIISC)

In cooperation with
Korea Information Security Agency
(KISA)

Under the patronage of the
Ministry of Information and Communication (MIC), Korea

General Chair

Kil-Hyun Nam (President of KIISC, Korea)

Technical Program Committee

Zongduo Dai (Academica Sinica, P.R.C.)
Ed Dawson (Queensland University of Technology, Australia)
Tzonelih Hwang (National Cheng-Kung University, Taiwan, R.O.C.)
Chul Kim (Kwangwoon University, Korea)
Kwangjo Kim (Information and Communication University, Korea)
Kaoru Kurosawa (Tokyo Institute of Technology, Japan)
Kwok-Yan Lam (National University of Singapore)
Koung Goo Lee (KISA, Korea)
Pil Joong Lee (Pohang University of Science & Technology, Korea)
Chae Hoon Lim (Future Systems Incorporation, Korea)
Jong In Lim (Korea University, Korea)
Chris Mitchell (University of London, U.K.)
Sang Jae Moon (Kyungpook National University, Korea)
Kaisa Nyberg (Nokia Research Center, Finland)
Eiji Okamoto (JAIST, Japan)
Tatsuaki Okamoto (NTT, Japan)
Choon Sik Park (ETRI, Korea)
Sung Jun Park (KISA, Korea)
Bart Preneel (Katholieke Universiteit Leuven, Belgium)
Dong Ho Won (Sungkyunkwang University, Korea)
Heung Youl Youm (Soonchunhyan University, Korea)
Moti Yung (CertCo, U.S.A.)
Yuliang Zheng (Monash University, Australia)

Organizing Committee

Jong In Lim (Korea University)
Sang Kyu Park (HanYang University)
Ha Bong Chung (HongIk University)
Dong Hoon Lee (Korea University)
Sang Jin Lee (Korea University)
Howang Bin Ryou (KwangWoon University)
Seok Woo Kim (HanSei University)
Yong Rak Choi (Taejon University)
Jae Moung Kim (ETRI)
Hong Sub Lee (KISA)
Seung Joo Han (ChoSun University)
Min Surp Rhee (DanKook University)
Seog Pal Cho (SeongGyul University)
Kyung Seok Lee (KIET)
Jong Seon No (Seoul National University)

Table of Contents

Invited Talk

On Provable Security for Conventional Cryptography 1
Serge Vaudenay (Ecole Polytechnique Federale de Lausanne)

Cryptanalysis and Cryptographic Design

Correlation Properties of the Bluetooth Combiner Generator 17
Miia Hermelin and Kaisa Nyberg (Nokia Research Center, Helsinki)

Preventing Double-Spent Coins from Revealing User's Whole Secret 30
DaeHun Nyang and JooSeok Song (Department of Computer Science, Yonsei University)

On the Optimal Diffusion Layers with Practical Security against Differential and Linear Cryptanalysis 38
Ju-Sung Kang and Choonsik Park (Electronics and Telecommunications Resaerch Center, Taejon) Sangjin Lee and Jong-In Lim (Department of Mathematics, Korea University, Korea)

Non-linear Complexity of the Naor–Reingold Pseudo-random Function 53
William D. Banks (Department of Mathematics, University of Missouri, Columbia), Frances Griffin (Department of Mathematics, Macquarie University, Sydney), Daniel Lieman (Department of Mathematics, University of Missouri, Columbia), and Igor E. Shparlinski (Department of Computing, Macquarie University, Sydney)

Cryptographic Theory and Computation Complexity

Relationships between Bent Functions and Complementary Plateaued Functions 60
Yuliang Zheng (School of Compting & Information Techology, Monash University) and Xian-Mo Zhang (University of Wollongong)

A Technique for Boosting the Security of Cryptographic Systems with One-Way Hash Functions 76
Takeshi Koshiba (Telecommunications Advancement Organization of Japan)

Over $\mathbf{F}_p$ vs. over $\mathbf{F}_{2^n}$ and on Pentium vs. on Alpha in Software Implementation of Hyperelliptic Curve Cryptosystems 82
Yasuyuki Sakai (Mitsubishi Electric Corporation) and Kouichi Sakurai (Kyushu University)

Speeding Up Elliptic Scalar Multiplication with Precomputation 102
Chae Hoon Lim and Hyo Sun Hwang (Information and CommunicationsResearch Center, Future Systems Inc.)

Cryptographic Protocol and Authentication Design

Why Hierarchical Key Distribution Is Appropriate for Multicast Networks 120
Chandana Gamage, Jussipekka Leiwo, and Yuliang Zheng (Peninsula School of Computing and Information Technology, Monash University)

Secure Selection Protocols 132
Kapali Viswanathan, Colin Boyd, and Ed Dawson (Information Security Research Centre, Queensland University of Technology)

Efficient 3-Pass Password-Based Key Exchange Protocol with Low Computational Cost for Client 147
Hyoungkyu Lee, Dongho Won (Information and Communications Security Laboratory, School of Electrical and Computer Engineering, Sungkyunkwan University), Kiwook Sohn (Electronics and Telecommunications Research Institute, Taejon), and Hyoungkyu Yang (Division of Computer Science, Electronics, and Industrial Engineering, Kangnam University)

A 2-Pass Authentication and Key Agreement Protocol for Mobile Communications 156
Kook-Heui Lee, Sang-Jae Moon (School of Electronic and Electrical Engineering, Kyungpook National University), Won-Young Jeong and Tae-Geun Kim (Access Network Resaerch Laboratory, Korea Telecom)

Digital Signature and Secret Sharing Scheme

Verifiable Secret Sharing and Time Capsules 169
Josef Pieprzyk (School of Information Technologies and Computer Science, University of Wollongong) and Eiji Okamoto (Center for Cryptography, Computer and Network Security, University of Wisconsin)

A New Approach to Robust Threshold RSA Signature Schemes 184
Rei Safavi-Naini (School of IT and CS, University of Wollongong), Huaxiong Wang, and Kwok-Yan Lam (Department of Computer Science, National University of Singapore)

On Threshold RSA-Signing with no Dealer 197
Shingo Miyazaki (Toshiba Corporation, System Integration Technology Center), Kouichi Sakurai (Kyushu University, Department of Computer Science), and Moti Yung (CertCo, NY)

A New Approach to Efficient Verifiable Secret Sharing for Threshold KCDSA Signature 208
Ho-Sun Yoon and Heung-Youl Youm (Department of Electrical and Electronic Engineering, College of Engineering, Soonchunhyang University)

Electronic Cash, Application, Implementation

A Hardware-Oriented Algorithm for Computing in Jacobians and Its Implementation for Hyperelliptic Curve Cryptosystems 221
Tetsuya Tamura IMB Research, Tokyo Research Laboratory, IBM Japan Ltd.), Kouichi Sakurai (Kyushu University), and Tsutomu Matsumoto (Yokohama-shi, Kanagawa)

A Security Design for a Wide-Area Distributed System 236
Jussipekka Leiwo, Christoph Hänle, Philip Homburg, Andrew S. Tanenbaum (Vrije Universiteit, Faculty of Sciene, Amsterdam), and Chandana Gamage (Monash University)

Self-Escrowed Public-Key Infrastructures 257
Pascal Paillier (Cryptography Group, Gemplus) and Moti Yung (CertCo, NY)

Electronic Funds Transfer Protocol Using Domain-Verifiable Signcryption Scheme 269
Moonseog Seo and Kwangjo Kim (ICU, Taejon)

Author Index 279