Lecture Notes in Computer Science 2015
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

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

Dongho Won (Ed.)

Information Security and Cryptology – ICISC 2000

Third International Conference
Seoul, Korea, December 8-9, 2000
Proceedings

Springer

Volume Editors

Dongho Won
Sungkyunkwan University, School of Electronical and Computer Engineering
300 Chunchun-dong, Jangan-gu, Suwon, Kyonggi, Korea
E-mail: dhwon@simsan.skku.ac.kr

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information security and cryptology : third international conference ; proceedings / ICISC 2000, Seoul, Korea, December 8 - 9, 2000. Dongho Won (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 2001
(Lecture notes in computer science ; Vol. 2015)
ISBN 3-540-41782-6

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, F.2.1, C.2, J.1

ISSN 0302-9743
ISBN 3-540-41782-6 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de
© Springer-Verlag Berlin Heidelberg 2001
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Stefan Sossna
Printed on acid-free paper   SPIN: 10782183   06/3142   5 4 3 2 1 0

Preface

I would like to welcome all the participants to the 3rd International Conference on Information Security and Cryptology (ICISC 2000). It is sponsored by the Korea Institute of Information Security and Cryptology (KIISC) and is being held at Dongguk University in Seoul, Korea from December 8 to 9, 2000. This conference aims at providing a forum for the presentation of new results in research, development, and application in information security and cryptology. This is also intended to be a place where research information can be exchanged.

The Call for Papers brought 56 papers from 15 countries and 20 papers will be presented in five sessions. As was the case last year the review process was totally blind and the anonymity of each submission was maintained. The 22 TPC members finally selected 20 top-quality papers for presentation at ICISC 2000.

I am very grateful to the TPC members who devoted much effort and time to reading and selecting the papers. We also thank the experts who assisted the TPC in evaluating various papers and apologize for not including their names here. Moreover, I would like to thank all the authors who submitted papers to ICISC 2000 and the authors of accepted papers for their preparation of camera-ready manuscripts. Last but not least, I thank my student, Joonsuk Yu, who helped me during the whole process of preparation for the conference.

I look forward to your participation and hope you will find ICISC 2000 a truly rewarding experience.

December 2000 Dongho Won

Organization

The 3rd International Conference on Information Security and Cryptology (ICISC 2000) is organized and sponsored by the Korea Institute of Information Security and Cryptology (KIISC).

Executive Committee

Kil Hyun Nam	General Chair (Presient of KIISC, Korea)
Dong Ho Won	TPC chair (Sungkyunkwan University, Korea)
Jae Ho Shin	Organizing Chair (Dongguk University, Korea)

Technical Program Committee

Dong Ho Won	Sungkyunkwan University, Korea
Zongduo Dai	Academia Sinica, P.R.C.
Ed Dawson	Queensland University of Technology, Australia
Chul Kim	Kwangwoon University, Korea
Kwang Jo Kim	Information and Communications University, Korea
Kaoru Kurosawa	Tokyo Inst. of Tech., Japan
Kwok-Yan Lam	National University of Singapore, Singapore
Kyoung Goo Lee	KISA, Korea
Pil Joong Lee	Pohang University of Sci. and Tech., Korea
Chae Hoon Lim	Future System Inc., Korea
Masahiro Mambo	Tohoku University, Japan
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	Toho University, Japan
Tatsuaki Okamoto	NTT, Japan
Choon Sik Park	ETRI, Korea
Sung Jun Park	BCQRE CO., LTD, Korea
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Heung Youl Youm	Soonchunhyang University, Korea
Moti Yung	CertCo, U.S.A.
Yuliang Zheng	Monash University, Australia

Organizing Committee

Jae Ho Shin	Dongguk University, Korea
Chee Sun Won	Dongguk University, Korea
Sang Kyu Park	Hanyang University, Korea
Ha Bong Chung	Hongik University, Korea
Dong Hoon Lee	Korea University, Korea
Jae Jin Lee	Dogguk University, Korea
Howang Bin Ryou	Kwangwoon University, Korea
Seok Woo Kim	Hansei University, Korea
Yong Rak Choi	Taejon University, Korea
Hyun Sook Cho	ETRI, Korea
Hong Sub Lee	KISA, Korea
Seung Joo Han	Chosun University, Korea
Min Surp Rhee	Dankook University, Korea
Seog Pal Cho	Seonggul University, Korea
Kyung Seok Lee	KIET, Korea
Joo Seok Song	Yonsei University, Korea
Jong Seon No	Seoul National University, Korea
Tai Myoung Chung	Sungkyunkwan University, Korea

Sponsoring Institutions

MIC (Ministry of Information and Communication), Korea
IITA (Institute of Information Technology Assessment), Korea
KISA (Korea Information Security Agency, Korea
Dongguk University, Korea
The Electronic Times, Korea

Table of Contents

A Note on the Higher Order Differential Attack of Block Ciphers with Two-Block Structures 1
Ju-Sung Kang, Seongtaek Chee, Choonsik Park (Department of Basic Technology, NSRI, Korea)

On the Strength of KASUMI without FL Functions against Higher Order Differential Attack 14
Hidema Tanaka, Chikashi Ishii, Toshinobu Kaneko (Science University of Tokyo, Japan)

On MISTY1 Higher Order Differential Cryptanalysis 22
Steve Babbage (Vodafone Ltd, England), Laurent Frisch (France Télécom Recherche et Développement, France)

Difference Distribution Attack on DONUT and Improved DONUT 37
Dong Hyeon Cheon, Seok Hie Hong, Sang Jin Lee (Center for Information and Security Technologies, Korea University, Korea), Sung Jae Lee, Kyung Hwan Park, Seon Hee Yoon (Korea Information Security Agency, Korea)

New Results on Correlation Immunity 49
Yuliang Zheng (Monash University, Australia), Xian-Mo Zhang (The University of Wollongong, Australia)

Elliptic Curves and Resilient Functions 64
Jung Hee Cheon (Mathematics Department, Brown University, USA, and Securepia, Korea), Seongtaek Chee (NSRI, Korea)

Fast Universal Hashing with Small Keys and No Preprocessing: The PolyR Construction 73
Ted Krovetz (Department of Computer Science, University of California, USA), Phillip Rogaway (Department of Computer Science, Chiang Mai University, Thailand)

Characterization of Elliptic Curve Traces under FR-Reduction 90
Atsuko Miyaji, Masaki Nakabayashi, Shunzo Takano (Japan Advanced Institute of Science and Technology, Japan)

A Multi-party Optimistic Non-repudiation Protocol 109
Olivier Markowitch, Steve Kremer (Computer Science Department, Université Libre de Bruxelles, Belgium)

Secure Matchmaking Protocol 123
Byoungcheon Lee, Kwangjo Kim (Information and Communications University, Korea)

An Improved Scheme of the Gennaro-Krawczyk-Rabin Undeniable Signature System Based on RSA ... 135
Takeru Miyazaki (Kyushu Institute of Technology, Japan)

Efficient and Secure Member Deletion in Group Signature Schemes ... 150
Hyun-Jeong Kim, Jong In Lim, Dong Hoon Lee (Center for Information Security Technologies, Korea University, Korea)

An Efficient and Practical Scheme for Privacy Protection in the E-Commerce of Digital Goods ... 162
Feng Bao, Robert H. Deng, Peirong Feng (Kent Ridge Digital Labs, Singapore)

An Internet Anonymous Auction Scheme ... 171
Yi Mu, Vijay Varadharajan (School of Computing and IT, University of Western Sydney, Australia)

Efficient Sealed-Bid Auction Using Hash Chain ... 183
Koutarou Suzuki, Kunio Kobayashi, Hikaru Morita (NTT Laboratories, Japan)

Micropayments for Wireless Communications ... 192
DongGook Park (Access Network Laboratory, Korea Telecom, Korea and Queensland University of Technology, Australia), Colin Boyd, Ed Dawson (Information Security Research Centre, Queensland University of Technology, Australia)

Cryptographic Applications of Sparse Polynomials over Finite Rings ... 206
William D. Banks (Department of Mathematics, University of Missouri, USA), Daniel Lieman (Department of Mathematics, University of Georgia, USA), Igor E. Shparlinski, Van Thuong To (Department of Computing, Macquarie University, Australia)

Efficient Anonymous Fingerprinting of Electronic Information with Improved Automatic Identification of Redistributors ... 221
Chanjoo Chung, Seungbok Choi, Dongho Won (School of Electrical and Computer Engineering, Sungkyunkwan University, Korea), Youngchul Choi (BCQRE Co., Korea)

Hash to the Rescue: Space Minimization for PKI Directories ... 235
Adam Young (Columbia University, USA), Moti Yung (CertCo, USA)

A Design of the Security Evaluation System for Decision Support in the Enterprise Network Security Management ... 246
Jae Seung Lee, Sang Choon Kim, Seung Won Sohn (Information Security Technology Division, ETRI, Korea)

Author Index ... 261