

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

New York University, NY, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Dengguo Feng Dongdai Lin
Moti Yung (Eds.)

Information Security and Cryptology

First SKLOIS Conference, CISC 2005
Beijing, China, December 15-17, 2005
Proceedings



Springer

Volume Editors

Dengguo Feng
Dongdai Lin
Chinese Academy of Sciences, Institute of Software
State Key Laboratory of Information Security
Beijing, 100080, P. R. China
E-mail: {feng,ddlin}@is.iscas.ac.cn

Moti Yung
RSA Laboratories and Columbia University
Computer science Department
Room 464, S.W. Mudd Building, New York, NY 10027, USA
E-mail: moti@cs.columbia.edu

Library of Congress Control Number: 2005937143

CR Subject Classification (1998): E.3, D.4.6, F.2.1, C.2, J.1, C.3, K.4.4, K.6.5

ISSN 0302-9743
ISBN-10 3-540-30855-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-30855-3 Springer 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. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springeronline.com

© Springer-Verlag Berlin Heidelberg 2005
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11599548 06/3142 5 4 3 2 1 0

Preface

The first SKLOIS Conference on Information Security and Cryptography (CISC 2005) was organized by the State Key Laboratory of Information Security of the Chinese Academy of Sciences. It was held in Beijing, China, December 15-17, 2005 and was sponsored by the Institute of Software, the Chinese Academy of Sciences, the Graduate School of the Chinese Academy of Sciences and the National Science Foundation of China. The conference proceedings, representing invited and contributed papers, are published in this volume of Springer's Lecture Notes in Computer Science (LNCS) series.

The area of research covered by CISC has been gaining importance in recent years, and a lot of fundamental, experimental and applied work has been done, advancing the state of the art. The program of CISC 2005 covered numerous fields of research within the general scope of the conference.

The International Program Committee of the conference received a total of 196 submissions (from 21 countries). Thirty-three submissions were selected for presentation as regular papers and are part of this volume. In addition to this track, the conference also hosted a short-paper track of 32 presentations that were carefully selected as well. All submissions were reviewed by experts in the relevant areas and based on their ranking and strict selection criteria the papers were selected for the various tracks. We note that stricter criteria were applied to papers co-authored by program committee members. We further note that, obviously, no member took part in influencing the ranking of his or her own submissions. In addition to the contributed regular papers, this volume contains the two invited papers by Serge Vaudenay and Giovanni Di Crescenzo.

Many people and organizations helped in making the conference a reality. We would like to take this opportunity to thank the Program Committee members and the external experts for their invaluable help in producing the conference program. We would like to thank the Organizing Committee members, the Co-chairs Dongdai Lin and Chunkun Wu, and the members Jiwu Jing and Wenling Wu. Dongdai Lin also served as a "Super Program Chair", organizing the electronic program discussions and coordinating the decision making process. We thank the various sponsors and, last but not least, we wish to thank all the authors who submitted papers to the conference, the invited speakers, the session chairs and all the conference attendees.

CISC 2005

First SKLOIS Conference on Information Security and Cryptology

Beijing, China
December 15-17, 2005

Sponsored and organized by
State Key Laboratory of Information Security
(Chinese Academy of Sciences)

Program Chairs

Dengguo Feng
Moti Yung

SKLOIS, Chinese Academy of Sciences, China
RSA Labs and Columbia University, USA

Program Committee

Dan Bailey
Feng Bao
Carlo Blundo
Felix Brandt
Ahto Buldas
YoungJu Choie
Zongduo Dai
George Davida
Ed Dawson
Cunsheng Ding
Keqin Feng
Keith Frikken
Jun Furukawa
Guang Gong
Jiwu Huang
Kwangjo Kim
Xuejia Lai
Dongdai Lin
Mulan Liu
Wenbo Mao
Tsutomu Matsumoto
Sjouke Mauw
Bodo Moller
Svetla Nikova
Thomas Pornin

RSA Laboratory, USA
Institute for Infocomm Research, Singapore
University of Salerno, Italy
Stanford University, USA
Tallin Technical University, Estonia
POSTECH, Korea
GSCAS, Chinese Academy of Sciences, China
UWM, USA
QUT, Australia
HKUST, Hong Kong, China
Tsinghua University, China
Purdue University, USA
NEC, Japan
University of Waterloo, Canada
Zhongshan University, China
ICU, Korea
Shanghai Jiaotong University, China
SKLOIS, Chinese Academy of Sciences, China
AMSS, CAS, China
Hewlett-Packard Labs, UK
Yokohama National University, Japan
EUT, Netherlands
Calgary, Canada
K.U. Leuven, Belgium
Cryptolog, France

VIII Organization

Michel Riguidel	ENST, France
Eiji Okamoto	Tsukuba University, Japan
Duong Hieu Phan	ENS, France
Bimal Roy	Indian Statistical Institute, India
Ahmad-Reza Sadeghi	Bochum, Germany
Kouichi Sakurai	Kyushu University, Japan
Tom Shrimpton	Portland State University, USA
Willy Susilo	University of Wollongong, Australia
Vijay Varadharajan	Macquarie, Australia
Xiaoyun Wang	Shandong University, China
Chuan-kun Wu	SKLOIS, Chinese Academy of Science, China
Yixian Yang	BUPT, China
Huanguo Zhang	Wuhan University, China
Yuliang Zheng	UNCC, USA
Hong Zhu	Fudan University, China
Yuefei Zhu	Information Engineering University, China

Organizing Committee

Dongdai LIN (Co-chair)	SKLOIS, Chinese Academy of Sciences, China
Chuankun Wu (Co-chair)	SKLOIS, Chinese Academy of Sciences, China
Jiwu JING	SKLOIS, Chinese Academy of Sciences, China
Wenling WU	SKLOIS, Chinese Academy of Sciences, China

Table of Contents

Invited Talks

On Bluetooth Repairing: Key Agreement Based on Symmetric-Key Cryptography <i>Serge Vaudenay</i>	1
You Can Prove So Many Things in Zero-Knowledge <i>Giovanni Di Crescenzo</i>	10

Identity Based Cryptography

Improvements on Security Proofs of Some Identity Based Encryption Schemes <i>Rui Zhang, Hideki Imai</i>	28
An ID-Based Verifiable Encrypted Signature Scheme Based on Hess's Scheme <i>Chunxiang Gu, Yuefei Zhu</i>	42
ID-Based Signature Scheme Without Trusted PKG <i>Jian Liao, Junfang Xiao, Yinghao Qi, Peiwei Huang, Mentian Rong</i>	53

Security Modelling

Specifying Authentication Using Signal Events in CSP <i>Siraj A. Shaikh, Vicky J. Bush, Steve A. Schneider</i>	63
Modeling RFID Security <i>Xiaolan Zhang, Brian King</i>	75

Systems Security

Enforcing Email Addresses Privacy Using Tokens <i>Roman Schlegel, Serge Vaudenay</i>	91
Efficient Authentication of Electronic Document Workflow <i>Yongdong Wu</i>	101

Signature Schemes

Practical Strong Designated Verifier Signature Schemes Based on Double Discrete Logarithms <i>Raylin Tso, Takeshi Okamoto, Eiji Okamoto</i>	113
Efficient Group Signatures from Bilinear Pairing <i>Xiangguo Cheng, Huafei Zhu, Ying Qiu, Xinmei Wang</i>	128
Enhanced Aggregate Signatures from Pairings <i>Zuhua Shao</i>	140
Constructing Secure Proxy Cryptosystem <i>Yuan Zhou, Zhenfu Cao, Zhenchuan Chai</i>	150

Symmetric Key Mechanisms

Towards a General RC4-Like Keystream Generator <i>Guang Gong, Kishan Chand Gupta, Martin Hell, Yassir Nawaz</i>	162
HCTR: A Variable-Input-Length Enciphering Mode <i>Peng Wang, Dengguo Feng, Wenling Wu</i>	175
The k th-Order Quasi-Generalized Bent Functions over Ring Z_p <i>Jihong Teng, Shiqu Li, Xiaoying Huang</i>	189
A Fast Algorithm for Determining the Linear Complexity of Periodic Sequences <i>Shimin Wei, Guolong Chen, Guozhen Xiao</i>	202

Zero-Knowledge and Secure Computations

An Unbounded Simulation-Sound Non-interactive Zero-Knowledge Proof System for NP <i>Hongda Li, Bao Li</i>	210
An Improved Secure Two-Party Computation Protocol <i>Yu Yu, Jussipekka Leiwo, Benjamin Premkumar</i>	221

Threshold Cryptography

Security Analysis of Some Threshold Signature Schemes and Multi-signature Schemes <i>Tianjie Cao, Dongdai Lin</i>	233
--	-----

ID-Based Threshold Unsignryption Scheme from Pairings <i>Fagen Li, Juntao Gao, Yupu Hu</i>	242
---	-----

Intrusion Detection Systems

Improvement of Detection Ability According to Optimum Selection of Measures Based on Statistical Approach <i>Gil-Jong Mun, Yong-Min Kim, DongKook Kim, Bong-Nam Noh</i>	254
--	-----

The Conflict Detection Between Permission Assignment Constraints in Role-Based Access Control <i>Chang-Joo Moon, Woojin Paik, Young-Gab Kim, Ju-Hum Kwon</i>	265
---	-----

Toward Modeling Lightweight Intrusion Detection System Through Correlation-Based Hybrid Feature Selection <i>Jong Sou Park, Khaja Mohammad Shazzad, Dong Seong Kim</i>	279
---	-----

Protocol Cryptanalysis

Security Analysis of Three Cryptographic Schemes from Other Cryptographic Schemes <i>Sherman S.M. Chow, Zhengjun Cao, Joseph K. Liu</i>	290
--	-----

An Effective Attack on the Quantum Key Distribution Protocol Based on Quantum Encryption <i>Fei Gao, Su-Juan Qin, Qiao-Yan Wen, Fu-Chen Zhu</i>	302
--	-----

ECC Algorithms

A Remark on Implementing the Weil Pairing <i>Cheol Min Park, Myung Hwan Kim, Moti Yung</i>	313
---	-----

Efficient Simultaneous Inversion in Parallel and Application to Point Multiplication in ECC <i>Pradeep Kumar Mishra</i>	324
--	-----

Applications

Key Management for Secure Overlay Multicast <i>Jong-Hyuk Roh, Kyoong-Ha Lee</i>	336
--	-----

Design and Implementation of IEEE 802.11i Architecture for Next Generation WLAN
Duhyun Bae, Jiho Kim, Sehyun Park, Ohyoung Song 346

Automatic Alignment of Fingerprint Features for Fuzzy Fingerprint Vault
Yongwha Chung, Daesung Moon, Sungju Lee, Seunghwan Jung, Taehae Kim, Dosung Ahn 358

Secret Sharing

Classification of Universally Ideal Homomorphic Secret Sharing Schemes and Ideal Black-Box Secret Sharing Schemes
Zhanfei Zhou 370

New Methods to Construct Cheating Immune Multisecret Sharing Scheme
Wen Ping Ma, Fu Tai Zhang 384

Denial of Service Attacks

Detection of Unknown DoS Attacks by Kolmogorov-Complexity Fluctuation
Takayuki Furuya, Takahiro Matsuzaki, Kanta Matsuura 395

MIPv6 Binding Update Protocol Secure Against Both Redirect and DoS Attacks
Hyun-Sun Kang, Chang-Seop Park 407

Author Index 419