Lecture Notes in Computer Science 3822

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

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

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.

December 2005 Dengguo Feng and Moti Yung

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

Program Committee

Dan Bailey	RSA Laboratory, USA
Feng Bao	Institute for Infocomm Research, Singapore
Carlo Blundo	University of Salerno, Italy
Felix Brandt	Stanford University, USA
Ahto Buldas	Tallin Technical University, Estonia
YoungJu Choie	POSTECH, Korea
Zongduo Dai	GSCAS, Chinese Academy of Sciences, China
George Davida	UWM, USA
Ed Dawson	QUT, Australia
Cunsheng Ding	HKUST, Hong Kong, China
Keqin Feng	Tsinghua University, China
Keith Frikken	Purdue University, USA
Jun Furukawa	NEC, Japan
Guang Gong	University of Waterloo, Canada
Jiwu Huang	Zhongshan University, China
Kwangjo Kim	ICU, Korea
Xuejia Lai	Shanghai Jiaotong University, China
Dongdai Lin	SKLOIS, Chinese Academy of Sciences, China
Mulan Liu	AMSS, CAS, China
Wenbo Mao	Hewlett-Packard Labs, UK
Tsutomu Matsumoto	Yokohama National University, Japan
Sjouke Mauw	EUT, Netherlands
Bodo Moller	Calgary, Canada
Svetla Nikova	K.U. Leuven, Belgium
Thomas Pornin	Cryptolog, France

Michel Riguidel	ENST, France
Eiji Okamato	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

Signature Schemes

Symmetric Key Mechanisms

Zero-Knowledge and Secure Computations

Threshold Cryptography

Intrusion Detection Systems

Protocol Cryptanalysis

ECC Algorithms

Applications

Secret Sharing

Denial of Service Attacks