Lecture Notes in Computer Science 6151

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

Feng Bao Moti Yung Dongdai Lin
Jiwu Jing (Eds.)

Information Security and Cryptology

5th International Conference, Inscrypt 2009
Beijing, China, December 12-15, 2009
Revised Selected Papers

Springer

Volume Editors

Feng Bao
Institute for Infocomm Research
1 Fusionopolis Way, #19-01 Connexis, South Tower, Singapore 138632, Singapore
E-mail: baofeng@i2r.a-star.edu.sg

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

Dongdai Lin
SKLOIS, Chinese Academy of Sciences, Institute of Software
Beijing 100190, China
E-mail: ddlin@is.iscas.ac.cn

Jiwu Jing
SKLOIS, Graduate University of Chinese Academy of Sciences
19A Yuquan Road, Beijing 100049, China
E-mail: jing@is.ac.cn

Library of Congress Control Number: 2010936095

CR Subject Classification (1998): C.2, K.6.5, E.3, D.4.6, J.1, H.4

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-16341-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-16341-8 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

The 5th China International Conference on Information Security and Cryptology (Inscrypt 2009) was co-organized by the State Key Laboratory of Information Security and by the Chinese Association for Cryptologic Research in cooperation with the International Association for Cryptologic Research (IACR). The conference was held in Beijing, China, in the middle of December, and was further sponsored by the Institute of Software, the Graduate University of the Chinese Academy of Sciences and the National Natural Science Foundations of China. The conference is a leading annual international event in the area of cryptography and information security taking place in China. The scientific program of the conference covered all areas of current research in the field, with sessions on central areas of cryptographic research and on many important areas of information security. The conference continues to get the support of the entire international community, reflecting on the fact that the research areas covered by Inscrypt are important to modern computing, where increased security, trust, safety and reliability are required.

The international Program Committee of Inscrypt 2009 received a total of 147 submissions from more than 20 countries and regions, from which only 32 submissions were selected for presentation, 22 of which in the regular papers track and 10 submissions in the short papers track. All anonymous submissions were reviewed by experts in the relevant areas and based on their ranking, technical remarks and strict selection criteria the papers were chosen for the various tracks. The selection to both tracks was a highly competitive process. We further note that due to the conference format, many good papers were regrettably not accepted. Besides the contributed papers, the program also included three invited presentations by Xiaoyun Wang, Roberts Deng and Moti Yung. The program also hosted two additional special tracks with presentations that are not included in these proceedings: one on White-Box Cryptography and Software Protection, and one on Post-Quantum Cryptography.

Inscrypt 2009 was made possible by the joint efforts of numerous people and organizations worldwide. We take this opportunity to thank the Program Committee members and the external experts they employed for their invaluable help in producing the conference program. We further thank the conference Organizing Committee, the various sponsors and the conference attendees. Last but not least, we express our great gratitude to all the authors who submitted papers to the conference, the invited speakers, the contributors to the special tracks and the Session Chairs.

December 2009

Feng Bao
Moti Yung

Inscrypt 2009

5th China International Conference on Information Security and Cryptology

Beijing, China December 12-15, 2009

Sponsored and organized by

State Key Laboratory of Information Security
(Chinese Academy of Sciences)
Chinese Association for Cryptologic Research

in cooperation with

International Association for Cryptologic Research

Steering Committee

Dengguo Feng	SKLOIS, Chinese Academy of Sciences, China
Dongdai Lin	SKLOIS, Chinese Academy of Sciences, China
Moti Yung	Google Inc. and Columbia University, USA
Chukun Wu	SKLOIS, Chinese Academy of Sciences, China

General Chairs

Dengguo Feng	SKLOIS, Chinese Academy of Sciences, China

Program Committee

Co-chairs

Feng Bao	Institute for Infocomm Research, Singapore
Moti Yung	Google Inc. and Columbia University, USA

Members

Rana Barua	Indian Statistical Institute, India
Zhenfu Cao	Shanghai Jiaotong University, China
Claude Carlet	Universite Paris 8, France
Luigi Catuogno	Ruhr University Bochum, Germany
Liqun Chen	HP Laboratories, UK
Ed Dawson	QUT, Australia
Robert Deng	SMU, Singapore
Xiaotie Deng	City University of Hong Kong, Hong Kong SAR

Jintai Ding	Cincinnati University, USA
Jean-Charles Faugere	INRIA, France
Keith Frikken	Miami University, USA
Alejandro Hevia	University of Chile, Chile
Dennis Hofheinz	CWI, The Netherlands
Brian King	Indiana University - Purdue University, USA
Miroslaw Kutylowski	Wroclaw University of Technology, Poland
Albert Levi	Sabanci University, Turkey
Chao Li	National University of Defence Technology, China
Hui Li	Xidian University, China
Jie Li	University of Tsukuba, Japan
Javier Lopez	University of Malaga, Spain
Xiapu Luo	Georgia Tech, USA
Masahiro Mambo	University of Tsukuba, Japan
Fabio Massacci	University of Trento, Italy
Yi Mu	University of Wollongang, Australia
Svetla Nikova	K.U. Leuven and University of Twente, Belgium
Peng Ning	North Carolina State University, USA
Adam O'Niell	Georgia Tech, USA
Raphael C.-W. Phan	Loughborough University, UK
Olivier Pereira	UCL, Belgium
Josef Pieprzyk	Macquarie University, Australia
Kui Ren	Illinois Institute of Technology, USA
Stelios Sidiroglou-Douskos	MIT, USA
Ioannis Stamatiou	University of Ioannina, Greece
Tsuyoshi Takagi	Future University, Japan
Toshiaki Tanaka	KDDI R&D Labs, Japan
Jacques Traore	Orange Labs, FT, France
Wen-Guey Tzeng	National Chiao Tung University, Taiwan
Daoshun Wang	Tsinghua University, China
Wenling Wu	Chinese Academy of Sciences, China
Yongdong Wu	I2R, Singapore
Shouhai Xu	University of Texas at San Antonio, USA
Yongjin Yeom	ETRI, Korea
Heung Youl Youm	SCH University, Korea
Meng Yu	Western Illinois University, USA
Erik Zenner	Technical University of Denmark
Rui Zhang	AIST, Japan
Yuliang Zheng	University of North Carolina at Charlotte, USA
Jianying Zhou	I2R, Singapore

Proceedings Co-editors

Feng Bao	Institute for Infocomm Research, Singapore
Moti Yung	Google Inc. and Columbia University, USA
Dongdai Lin	SKLOIS, Institute of Software, Chinese Academy of Sciences, China
Jiwu Jing	SKLOIS, Graduate University of Chinese Academy of Sciences, China

Organizing Committee

Co-chairs

Jiwu Jing	SKLOIS, Graduate University of Chinese Academy of Sciences, China
Zhijun Qiang	Chinese Association for Cryptologic Research, China

Members

Chuankun Wu	SKLOIS, Institute of Software, Chinese Academy of Sciences, China
Daren Zha	Graduate University, CAS, China
Xiaoyang Wen	Graduate University, CAS, China
Aihua Zhang	Graduate University, CAS, China

Workshop Chair

Dongdai Lin	SKLOIS, Institute of Software, Chinese Academy of Sciences, China

Publicity Chair

Huafei Zhu	Institute for Infocomm Research, Singapore

Website/Registration

Yicong Liu	Graduate University, CAS, China
Le Kang	Graduate University, CAS, China
Ying Qiu	Institute for Infocomm Research, Singapore

Conference Secretary

Daren Zha	Graduate University, CAS, China
Zongbin Liu	Graduate University, CAS, China

Table of Contents

Cryptanalysis

Signature and Signcryption

Key Exchange

Private Computations

Cipher Design and Analysis

Public Key Cryptography

Network and System Security

Hardware Security

Web Security