Lecture Notes in Computer Science 8567

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

Editorial Board

More information about this series at http://www.springer.com/series/7410

Dongdai Lin · Shouhuai Xu
Moti Yung (Eds.)

Information Security and Cryptology

9th International Conference, Inscrypt 2013 Guangzhou, China, November 27–30, 2013 Revised Selected Papers

Springer

Editors
Dongdai Lin
Chinese Academy of Sciences
Beijing
China

Moti Yung
Columbia University
New York, NY
USA

Shouhuai Xu
University of Texas
San Antonio, TX
USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
ISBN 978-3-319-12086-7 ISBN 978-3-319-12087-4 (eBook)
DOI 10.1007/978-3-319-12087-4

Library of Congress Control Number: 2014953264

LNCS Sublibrary: SL4 – Security and Cryptology

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This volume contains the papers presented at Inscrypt 2013: The Ninth China International Conference on Information Security and Cryptology held during November 27–30, 2013 in Guangzhou, China. Inscrypt 2013 was collocated with the 2013 Workshop on RFID and IOT Security (RFIDsec 2013 Asia), which was held on November 27, 2013. Since its inauguration in 2005, Inscrypt has become a well-recognized annual international forum for security researchers and cryptographers to exchange ideas.

The conference received 93 submissions. Each submission was reviewed by at least three, and mostly four Program Committee members. The Program Committee decided to accept 25 papers, including 4 short papers, and 1 full paper that was a merge of two submissions. The overall acceptance rate was, therefore, about 26.8 %. The program also included three invited talks.

Inscrypt 2013 was held in cooperation with the International Association of Cryptologic Research (IACR), and co-organized by the State Key Laboratory of Information Security (SKLOIS) of the Chinese Academy of Sciences (CAS), the Chinese Association for Cryptologic Research (CACR), and Guangzhou University. Inscrypt 2013 was partly supported by the Natural Science Foundation of China (NSFC), the Institute of Information Engineering (IIE) of the Chinese Academy of Sciences, and Guangzhou University. Inscrypt 2013 could not have been a success without the support of these organizations, and we sincerely thank them for their continued assistance and help.

We would also like to thank the authors who submitted their papers to Inscrypt 2013, and the conference attendees for their interest and support that made the conference possible. We thank the Organizing Committee for their time and efforts that allowed us to focus on selecting papers. We thank the Program Committee members and the external reviewers for their hard work in reviewing the submissions; the conference would not have been possible without their expert reviews. Last but not least, we thank the EasyChair system and its operators for making the entire process of the conference convenient.

November 2013

Dongdai Lin
Shouhuai Xu
Moti Yung

Inscrypt 2013

9th China International Conference on Information Security and Cryptology

Guangzhou, China
November 27–30, 2013

Sponsored and organized by

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

in cooperation with
International Association for Cryptologic Research

Conference Chair

Dingyi Pei	Guangzhou University, China

Conference Organizing Committee

Zhijun Qiang	Chinese Association for Cryptologic Research, China
Chunming Tang	Guangzhou University, China
Chuankun Wu	SKLOIS, Chinese Academy of Sciences, China

Program Co-chairs

Dongdai Lin	SKLOIS, Chinese Academy of Sciences, China
Shouhuai Xu	University of Texas at San Antonio, USA
Moti Yung	Google Inc. and Columbia University, USA

Program Committee

Guoqiang Bai	Tsinghua University, China
Elisa Bertino	Purdue University, USA
Zhenfu Cao	Shanghai Jiao Tong University, China
Bogdan Carbunar	Florida International University, USA
Kefei Chen	Shanghai Jiao Tong University, China

Liqun Chen	Hewlett-Packard Laboratories, UK
Zhong Chen	Peking University, China
Sherman S.M. Chow	Chinese University of Hong Kong, Hong Kong
Ed Dawson	Queensland University of Technology, Australia
Jintai Ding	University of Cincinnati, USA
Cunsheng Ding	Hong Kong University of Science and Technology, Hong Kong
Xuhua Ding	Singapore Management University, Singapore
Shlomi Dolev	Ben-Gurion University of the Negev, Israel
Yingfei Dong	University of Hawaii, USA
Lei Hu	SKLOIS Chinese Academy of Sciences, China
Miroslaw Kutylowski	Wrocław University of Technology, Poland
Xuejia Lai	Shanghai Jiao Tong University, China
Jiangtao Li	Intel Corporation, USA
Hui Li	Xidian University, China
Zhiqiang Lin	University of Texas at Dallas, USA
Donggang Liu	University of Texas at Arlington, USA
Peng Liu	Pennsylvania State University, USA
Di Ma	University of Michigan-Dearborn, USA
Subhamoy Maitra	Indian Statistical Institute, India
Florian Mendel	Graz University of Technology, Austria
Atsuko Miyaji	Japan Advanced Institute of Science and Technology, Japan
Yi Mu	University of Wollongong, Australia
Claudio Orlandi	Aarhus University, Denmark
Xinming Ou	Kansas State University, USA
Ludovic Perret	UPMC/LIP6 Inria/SALSA, France
Giuseppe Persiano	Università di Salerno, Italy
Bertram Poettering	Royal Holloway, University of London, UK
Kouichi Sakurai	Kyushu University, Japan
Nitesh Saxena	University of Alabama at Birmingham, USA
Jae Hong Seo	Myongji University, Republic of Korea
Claudio Soriente	ETH Zurich, Switzerland
Wen-Guey Tzeng	National Chiao Tung University, Taiwan
Yevgeniy Vahlis	AT&T Labs, USA
Xiaofeng Wang	Indiana University, USA
Wenling Wu	Institute of Software, Chinese Academy of Sciences, China
Huaxiong Wang	Nanyang Technological University, Singapore
Guilin Wang	University of Wollongong, Australia
Duncan Wong	City University of Hong Kong, Hong Kong
Maozhi Xu	Peking University, China
Danfeng Yao	Virginia Tech, USA
Chung-Huang Yang	National Kaohsiung Normal University, Taiwan
Yunlei Zhao	Fudan University, China
Fangguo Zhang	Sun Yat-sen University, China

Rui Zhang	Chinese Academy of Sciences, China
Hong-Sheng Zhou	University of Maryland, USA
Yuliang Zheng	UNC Charlotte, USA
Cliff Zou	University of Central Florida, USA
Giovanni Russello	The University of Auckland, New Zealand

External Reviewers

Adhikari, Avishek
Asghar, Muhammad Rizwan
Azimpurkivi, Mozhgan
Bai, Guoqiang
Bao, Zhenzhen
Barni, Mauro
Baum, Carsten
Chen, I-Te
Chen, Jiageng
Chen, Kai
Cheng, Chen-Mou
Chien, Hung-Yu
Dalla Preda, Mila
Ding, Yi
Eichlseder, Maria
Fan, Chun-I
Fan, Leo
Fiore, Dario
Fitzpatrick, Robert
Futa, Yuichi
Gao, Song
Gao, Wei
George, Wesley
Gligoroski, Danilo
Gong, Boru
Guo, Fuchun
Gupta, Aditi
Gupta, Kishan
Habibi, Mohammad
Han, Jinguang
Hanzlik, Lucjan
Huang, Jialin
Huang, Yun
Hwang, Ren Junn
Jhanwar, Mahabir Prasad
Jiao, Lin
Juang, Wen-Shenq
Kantarcioglu, Murat
Kubota, Ayumu
Kuo, Po-Chun
Lamberger, Mario
Langlois, Adeline
Lee, Hyung Tae
Li, Nan
Lin, Jiao
Liu, Zhen
Lomne, Victor
Long, Yu
Lv, Xixiang
Machado David, Bernardo
Mao, Xianping
Marson, Giorgia Azzurra
Ming, Tang
Mohamed, Manar
Mouha, Nicky
Mukherjee, Pratyay
Neupane, Ajaya
Nishide, Takashi
Panwar, Nisha
Paterson, Kenny
Pattuk, Erman
Polychroniadou, Antigoni
Qin, Baodong
Rao, Fang-Yu
Ren, Chuangang
Renault, Guenael
Schläffer, Martin
Shebaro, Bilal
Shirvanian, Maliheh
Shrestha, Babins
Snook, Michael
Song, Fang

Su, Chunhua
Su, Ming
Sun, Xiaoyan
Tang, Fei
Tang, Qiang
Tang, Ying-Kai
Tso, Raylin
Wang, Chih Hung
Wang, Kunpeng
Wang, Liangliang
Wang, Yanfeng
Wei, Puwen
Wu, Shenbao
Xagawa, Keita
Xiao, Gaoyao
Xu, Hong
Xue, Weijia
Yasunaga, Kenji
Yoneyama, Kazuki
Yuen, Tsz Hon
Zeitoun, Rina
Zeng, Xiangyong
Zhang, Cong
Zhang, Haibin
Zhang, Huiling
Zhang, Lei
Zhang, Su
Zhang, Tao
Zhao, Chang-An
Zhao, Fangming
Zhao, Mingyi
Zhao, Yongjun
Zhou, Xuhua

Contents

Computational Number Theory

Public Key Cryptography

Hash Function

Side-Channel and Leakage