

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, 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, Zürich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

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

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

ISBN 978-3-319-12086-7

DOI 10.1007/978-3-319-12087-4

ISSN 1611-3349 (electronic)

ISBN 978-3-319-12087-4 (eBook)

Library of Congress Control Number: 2014953264

LNCS Sublibrary: SL4 – Security and Cryptology

Springer Cham Heidelberg New York Dordrecht London

© Springer International Publishing Switzerland 2014

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

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
Mirosław 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
Fanguo Zhang	Sun Yat-sen University, China

Rui Zhang
 Hong-Sheng Zhou
 Yuliang Zheng
 Cliff Zou
 Giovanni Russello

Chinese Academy of Sciences, China
 University of Maryland, USA
 UNC Charlotte, USA
 University of Central Florida, USA
 The University of Auckland, New Zealand

External Reviewers

Adhikari, Avishek
 Asghar, Muhammad Rizwan
 Azimpurkivi, Mozghan
 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

Boolean Function and Block Cipher

A Note on Semi-bent and Hyper-bent Boolean Functions.	3
<i>Chunming Tang, Yu Lou, Yanfeng Qi, Maozhi Xu, and Baoan Guo</i>	
New Construction of Differentially 4-Uniform Bijections	22
<i>Claude Carlet, Deng Tang, Xiaohu Tang, and Qunying Liao</i>	
Automatic Security Evaluation of Block Ciphers with S-bP Structures Against Related-Key Differential Attacks	39
<i>Siwei Sun, Lei Hu, Ling Song, Yonghong Xie, and Peng Wang</i>	

Sequence and Stream Cipher

On the Key-Stream Periods Probability of Edon80	55
<i>Yunqing Xu</i>	
Cube Theory and Stable k -Error Linear Complexity for Periodic Sequences . . .	70
<i>Jianqin Zhou, Wanquan Liu, and Guanglu Zhou</i>	
Autocorrelation Values of New Generalized Cyclotomic Sequences of Order Six Over Z_{pq}	86
<i>Xinxin Gong, Bin Zhang, Dengguo Feng, and Tongjiang Yan</i>	

Applications: Systems and Theory

Automatic Detection and Analysis of Encrypted Messages in Malware	101
<i>Ruoxu Zhao, Dawu Gu, Juanru Li, and Yuanyuan Zhang</i>	
EAdroid: Providing Environment Adaptive Security for Android System	118
<i>Hongliang Liang, Yu Dong, Bin Wang, and Shuchang Liu</i>	
Supervised Usage of Signature Creation Devices.	132
<i>Przemysław Kubiak and Mirosław Kutylowski</i>	
A Practical Attack on <i>Patched</i> MIFARE Classic	150
<i>Yi-Hao Chiu, Wei-Chih Hong, Li-Ping Chou, Jintai Ding, Bo-Yin Yang, and Chen-Mou Cheng</i>	

Computational Number Theory

Omega Pairing on Hyperelliptic Curves	167
<i>Shan Chen, Kunpeng Wang, Dongdai Lin, and Tao Wang</i>	
Pairing Computation on Edwards Curves with High-Degree Twists	185
<i>Liangze Li, Hongfeng Wu, and Fan Zhang</i>	
The Gallant-Lambert-Vanstone Decomposition Revisited	201
<i>Zhi Hu and Maozhi Xu</i>	
Low-Weight Primes for Lightweight Elliptic Curve Cryptography on 8-bit AVR Processors	217
<i>Zhe Liu, Johann Großschädl, and Duncan S. Wong</i>	

Public Key Cryptography

Secure One-to-Group Communications Escrow-Free ID-Based Asymmetric Group Key Agreement.	239
<i>Lei Zhang, Qianhong Wu, Josep Domingo-Ferrer, Bo Qin, Sherman S.M. Chow, and Wenchang Shi</i>	
Security Model and Analysis of FHMVQ, Revisited	255
<i>Shengli Liu, Kouichi Sakurai, Jian Weng, Fangguo Zhang, and Yunlei Zhao</i>	
RSA-OAEP Is RKA Secure	270
<i>Dingding Jia, Bao Li, Xianhui Lu, and Yamin Liu</i>	
A Note on a Signature Building Block and Relevant Security Reduction in the Green-Hohenberger OT Scheme.	282
<i>Zhengjun Cao, Frederic Lafitte, and Olivier Markowitch</i>	

Hash Function

LHash: A Lightweight Hash Function	291
<i>Wenling Wu, Shuang Wu, Lei Zhang, Jian Zou, and Le Dong</i>	
Cryptanalysis of the Round-Reduced GOST Hash Function	309
<i>Jian Zou, Wenling Wu, and Shuang Wu</i>	

Side-Channel and Leakage

Multivariate Leakage Model for Improving Non-profiling DPA on Noisy Power Traces	325
<i>Suvadeep Hajra and Debdeep Mukhopadhyay</i>	

Partially Known Nonces and Fault Injection Attacks on SM2 Signature Algorithm	343
<i>Mingjie Liu, Jiazhe Chen, and Hexin Li</i>	

Application and System Security

Environment-Bound SAML Assertions: A Fresh Approach to Enhance the Security of SAML Assertions	361
<i>Kai Chen, Dongdai Lin, Li Yan, and Xin Sun</i>	
One-Time Programs with Limited Memory	377
<i>Konrad Durnoga, Stefan Dziembowski, Tomasz Kazana, and Michal Zajac</i>	
Cryptanalysis of Three Authenticated Encryption Schemes for Wireless Sensor Networks	395
<i>Xiaoqian Li, Peng Wang, Bao Li, and Zhelei Sun</i>	
Author Index	407