Lecture Notes in Computer Science 6584

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

Xuejia Lai Moti Yung Dongdai Lin (Eds.)

Information Security and Cryptology

6th International Conference, Inscrypt 2010
Shanghai, China, October 20-24, 2010
Revised Selected Papers

Springer

Volume Editors

Xuejia Lai
Shanghai Jiaotong University, Department of Computer Science and Engineering
Dongchuan Road 800, Shanghai 200240, China
E-mail: lai-xj@cs.sjtu.edu.cn

Moti Yung
Google Inc. and Columbia University, Computer Science Department
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

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-21517-9 e-ISBN 978-3-642-21518-6
DOI 10.1007/978-3-642-21518-6
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011928934

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

LNCS Sublibrary: SL 4 – Security and Cryptology

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

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

Preface

The 6th China International Conference on Information Security and Cryptology (Inscrypt 2010) was held in Shanghai, China, during October 20–23, 2010. The conference is a leading annual international event in the area of cryptography and information security taking place in China. Inscrypt continues to get the support of the entire international community, reflecting the fact that the research areas covered by the conference are important to modern computing, where increased security, trust, safety and reliability are required.

Inscrypt 2010 was co-organized by the State Key Laboratory of Information Security and by the Chinese Association for Cryptologic Research, in cooperation with Shanghai Jiaotong Univeristy and the International Association for Cryptologic Research (IACR). The conference was further sponsored by the Institute of Software, the Graduate University of the Chinese Academy of Science and the National Natural Science Foundations of China.

The scientific program of the conference covered all areas of current research in cryptography and security, with sessions on central subjects of cryptographic research and on some important subjects of information security. The international Program Committee of Inscrypt 2010 received a total of 125 submissions from more than 29 countries and regions, from which only 35 submissions were selected for presentation in the regular papers track and 13 submissions in the short papers track. Regular track papers appear in these proceedings volume. 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 to 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 two invited presentations by Bart Preneel and Moti Yung.

Inscrypt 2010 was made possible by a joint effort 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, and the session Chairs.

December 2010

Xuejia Lai
Moti Yung

Inscrypt 2010

6th China International Conference on Information Security and Cryptology

Shanghai, China October 20–23, 2010

Sponsored and organized by

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

in cooperation with

Shanghai Jiaotong University
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
Chuankun Wu	SKLOIS, Chinese Academy of Sciences, China

General Chair

Dengguo Feng	SKLOIS, Chinese Academy of Sciences, China

Program Committee

Co-chairs

Xuejia Lai	Shanghai Jiaotong University, China
Moti Yung	Google Inc. and Columbia University, USA

Members

Vladimir Anashin	Moscow State University, Russia
Frederik Armknecht	Institute for Computer Science at the University of Mannheim, Germany
Rana Barua	Indian Statistical Institute, Kolkata, India
Zhenfu Cao	Shanghai Jiaotong University, China
Claude Carlet	Université Paris 8, France

Luigi Catuogno	Università degli Studi di Salerno, Italy
Lily Chen	National Institute of Standards and Technology, USA
Liqun Chen	HP Laboratories, UK
Ed Dawson	QUT, Australia
Robert Deng	Singapore Management University, Singapore
Jintai Ding	Cincinnati University, USA
Jean-Charles Faugère	INRIA, France
Keith Frikken	Miami University, USA
Alejandro Hevia	University of Chile, Chile
James Hughes	Huawei North America, USA
Jiwu Jing	GUCAS, Chinese Academy of Sciences, China
Brian King	Indiana University-Purdue University, USA
Albert Levi	Sabanci University, Turkey
Chao Li	National University of Defence Technology, China
Peng Liu	Pennsylvania State University, USA
Javier Lopez	University of Malaga, Spain
Masahiro Mambo	University of Tsukuba, Japan
Atsuko Miyaji	Japan Advanced Institute of Science and Technology, Japan
Yi Mu	University of Wollongong, Australia
Peng Ning	North Carolina State University, USA
Olivier Pereira	Université Catholique de Louvain, Belgium
Ludovic Perret	LIP6, France
Svetla Petkova-Nikova	K.U. Leuven, Belgium and University of Twente, The Netherlands
Raphael Phan	Loughborough University, UK
Josef Pieprzyk	Macquarie University, Australia
Kui Ren	Illinois Institute of Technology, USA
Yannis Stamatiou	University of Ioannina, Greece
Tsuyoshi Takagi	Kyushu University, Japan
Jacques Traore	Orange Labs, France
Wen-Guey Tzeng	National Chiao Tung University, Taiwan
Daoshun Wang	Tsinghua University, China
Huaxiong Wang	Nanyang Technological University, Singapore
Wenling Wu	Institute of Software, CAS, China
Shouhai Xu	University of Texas at San Antonio, USA
Nong Ye	Arizona State University, USA
HeungYoul Youm	Soonchunhyang University, Korea
Meng Yu	Virginia Commonwealth University, USA
Erik Zenner	Technical University of Denmark
Rui Zhang	AIST, Japan
Yuliang Zheng	University of North Carolina at Charlotte, USA
Jianying Zhou	Institute for Infocomm Research, Singapore

Proceedings Co-editors

Xuejia Lai	Shanghai Jiaotong University, China
Moti Yung	Google Inc. and Columbia University, USA
Dongdai Lin	SKLOIS, Chinese Academy of Sciences, China

Organizing Committee

Co-chairs

Kefei Chen	Shanghai Jiaotong University, China
Chuankun Wu	SKLOIS, Chinese Academy of Sciences, China

Members

Feng Liu	Institute of Software, CAS, China
Yanfei Zheng	Shanghai Jiaotong University, China
Xianping Mao	Shanghai Jiaotong University, China

Publication Chair

Dongdai Lin	SKLOIS, Chinese Academy of Sciences, China

WEB Master

Jinyuan Tang	Institute of Software, CAS, China

Conference Secretary

Yi Qin	Institute of Software, CAS, China

Table of Contents

Encryption Schemes

New Constructions of Public-Key Encryption Schemes from Conjugacy Search Problems 1
Lihua Wang, Licheng Wang, Zhenfu Cao, Eiji Okamoto, and Jun Shao

On the CCA1-Security of Elgamal and Damgård's Elgamal 18
Helger Lipmaa

Online/Offline Identity-Based Signcryption Revisited 36
Joseph K. Liu, Joonsang Baek, and Jianying Zhou

Error-free, Multi-bit Non-committing Encryption with Constant Round Complexity 52
Huafei Zhu and Feng Bao

Stream Ciphers, Sequences and Elliptic Curves

A New Practical Key Recovery Attack on the Stream Cipher RC4 under Related-Key Model 62
Jiageng Chen and Atsuko Miyaji

An Efficient, Parameterized and Scalable S-box for Stream Ciphers 77
Sourav Das and Dipanwita RoyChowdhury

A Family of Binary Threshold Sequences Constructed by Using the Multiplicative Inverse 95
Zhixiong Chen, Xiangguo Cheng, and Chenhuang Wu

A Generalization of Verheul's Theorem for Some Ordinary Curves 105
Zhi Hu, Maozhi Xu, and Zhenghua Zhou

Secure Computing

On the Combinatorial Approaches of Computing Upper Bounds on the Information Rate of Secret Sharing Schemes 115
Zhanfei Zhou

Building Oblivious Transfer on Channel Delays 125
Paolo Palmieri and Olivier Pereira

Hash Functions

Variants of Multicollision Attacks on Iterated Hash Functions 139
Tuomas Kortelainen, Juha Kortelainen, and Kimmo Halunen

Hyper-Sbox View of AES-like Permutations: A Generalized Distinguisher 155
Shuang Wu, Dengguo Feng, Wenling Wu, and Bozhan Su

Preimage Attacks on Step-Reduced RIPEMD-128 and RIPEMD-160 ... 169
Chiaki Ohtahara, Yu Sasaki, and Takeshi Shimoyama

Pseudo-Cryptanalysis of Luffa 187
Keting Jia, Yvo Desmedt, Lidong Han, and Xiaoyun Wang

Distinguishing Attacks on LPMAC Based on the Full RIPEMD and Reduced-Step RIPEMD-{256, 320} 199
Gaoli Wang

Key Management

How to Construct Secure and Efficient Three-Party Password-Based Authenticated Key Exchange Protocols 218
Weijia Wang, Lei Hu, and Yong Li

Redesigning Group Key Exchange Protocol Based on Bilinear Pairing Suitable for Various Environments 236
Yvo Desmedt and Atsuko Miyaji

Multi-Factor Authenticated Key Exchange Protocol in the Three-Party Setting 255
Ying Liu, Fushan Wei, and Chuangui Ma

KALwEN+: Practical Key Management Schemes for Gossip-Based Wireless Medical Sensor Networks 268
Zheng Gong, Qiang Tang, Yee Wei Law, and Hongyang Chen

Determining Parameters of Key Predistribution Schemes via Linear Codes in Wireless Sensor Networks 284
Qi Chen, Dingyi Pei, and Junwu Dong

Digital Signatures

Fully-Secure and Practical Sanitizable Signatures 300
Junqing Gong, Haifeng Qian, and Yuan Zhou

Rigorous Security Requirements for Designated Verifier Signatures 318
Kazuki Yoneyama, Mebae Ushida, and Kazuo Ohta

Quasi-Dyadic CFS Signatures 336
Paulo S.L.M. Barreto, Pierre-Louis Cayrel, Rafael Misoczki, and Robert Niebuhr

Online/Offline Verification of Short Signatures 350
Yilian Zhang, Zhide Chen, and Fuchun Guo

Privacy and Algebraic Cryptanalysis

Acquiring Key Privacy from Data Privacy 359
Rui Zhang

Private Information Retrieval with a Trusted Hardware Unit – Revisited 373
Łukasz Krzywiecki, Mirosław Kutyłowski, Hubert Misztela, and Tomasz Strumiński

Algebraic Precomputations in Differential and Integral Cryptanalysis ... 387
Martin Albrecht, Carlos Cid, Thomas Dullien, Jean-Charles Faugère, and Ludovic Perret

A Note on Fast Algebraic Attacks and Higher Order Nonlinearities 404
Qichun Wang and Thomas Johansson

Hashing and Authentication

Comments and Improvements on Key-Exposure Free Chameleon Hashing Based on Factoring 415
Xiaofeng Chen, Haibo Tian, Fangguo Zhang, and Yong Ding

Quasi-Linear Cryptanalysis of a Secure RFID Ultralightweight Authentication Protocol 427
Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Raphael C.-W. Phan, Juan M.E. Tapiador, and Tieyan Li

Dwork-Naor ZAP and Its Application in Deniable Authentication, *Revisited* 443
Shaoquan Jiang

Hardware and Software Issues

Efficient Online/Offline Signatures with Computational Leakage Resilience in Online Phase 455
Fuchun Guo, Yi Mu, and Willy Susilo

Characterization of the Electromagnetic Side Channel in Frequency Domain 471
Olivier Meynard, Denis Réal, Sylvain Guilley, Florent Flament, Jean-Luc Danger, and Frédéric Valette

On Obfuscating Programs with Tamper-proof Hardware 487
Ning Ding and Dawu Gu

DepSim: A Dependency-Based Malware Similarity Comparison System 503
Yang Yi, Ying Lingyun, Wang Rui, Su Purui, and Feng Dengguo

Author Index 523