Lecture Notes in Computer Science 4990

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

Dingyi Pei Moti Yung Dongdai Lin
Chuankun Wu (Eds.)

Information Security and Cryptology

Third SKLOIS Conference, Inscrypt 2007
Xining, China, August 31–September 5, 2007
Revised Selected Papers

Springer

Volume Editors

Dingyi Pei
Guangzhou University
Institute of Information Security
Guangzhou, China
E-mail: gztcdpei@scut.edu.cn

Moti Yung
Google Inc., and Columbia University
Department of Computer Science
New York, NY, USA
E-mail: moti@cs.columbia.edu

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

Chuankun Wu
SKLOIS, Institute of Software
Chinese Academy of Sciences
Beijing, China
E-mail: ckwu@is.iscas.ac.cn

Library of Congress Control Number: Applied for

CR Subject Classification (1998): E.3, D.4.6, F.2.1, C.2, J.1, C.3, K.4.4, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-79498-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-79498-1 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12263486 06/3180 5 4 3 2 1 0

Preface

The Third SKLOIS Conference on Information Security and Cryptology (Inscrypt 2007) was organized by the State Key Laboratory of Information Security of the Chinese Academy of Sciences in cooperation with Qinhai University for Nationalities. This international conference was held in Xining, Qinhai Province of China, and was sponsored by the Institute of Software, the Chinese Academy of Sciences, the Graduate University of the Chinese Academy of Sciences and the National Natural Science Foundations of China.

By now, Inscrypt (the International SKLOIS Conference on Information Security and Cryptology) has become a tradition, and it is, in fact, a leading event in this area, which takes place annually in China. We are pleased with the continuous support by authors, committee members, reviewers, sponsors and organizers. Indeed, the research areas covered by Inscrypt are important, since modern computing (including communication infrastructures and applications) requires increased security, trust, safety and reliability. This need has motivated the research community worldwide to produce important fundamental, experimental and applied work in the wide areas of cryptography and information security research in recent years. Accordingly, the program of Inscrypt 2007 covered numerous fields of research within these general areas.

The international Program Committee of the conference received a total of 167 submissions from 21 countries and regions, from which only 43 submissions were selected for presentation, 33 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. We note also that reviews of submissions by committee members were hidden from their authors throughout the entire review process. We also note that due to the conference format, many good papers were regrettably not accepted.

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 thank the conference Organizing Committee, the various sponsors and the conference attendees. Last but not least, we also express our thanks to all the authors who submitted papers to the conference, the invited speakers and the session Chairs.

August/September 2007

Dingyi Pei
Moti Yung

Inscrypt 2007

Third SKLOIS Conference
on Information Security and Cryptology

Xining, Qinghai, China
August 31 - September 2, 2007

Sponsored and organized by

State Key Laboratory of Information Security
(Chinese Academy of Sciences)
and
Qinhai University for Nationalities

General Co-chairs

Dengguo Feng	SKLOIS, Chinese Academy of Sciences, China
Youyi Zhang	Qinhai University for Nationalities, China

Program Co-chairs

Dingyi Pei	Guangzhou University, China
Moti Yung	Google inc and Columbia University, USA

Program Committee

Feng Bao	I2R, Singapore
Rana Barua	Indian Statistical Institute, India
Lejla Betina	U.K. Leuven, Belgium
Emmanuel Bresson	DCSSI Crypto Lab, France
Bogdan Carbunar	Motorola Labs, USA
Robert H. Deng	SMU, Singapore
Cunsheng Ding	HKUST, Hong Kong, China
Marc Girault	France Telecom, France
Bok Min Goi	Multimedia University, Malaysia
Dieter Gollmann	TU Harburg, Germany
Goichiro Hanaoka	AIST, Japan
Tor Helleseth	Bergen University, Norway
Lei Hu	SKLOIS, Chinese Academy of Sciences, China
Stamatiou Iwannis	University of Patras, Greece
Hongxia Jin	IBM Almaden Research Center, USA
Vladimir Kolesnikov	Bell-Labs, USA
Xuejie Lai	Shanghai Jiaotong University, China

DongHoon Lee	Korea University, Korea
Benoit Libert	U.C. Louvain, Belgium
Dongdai Lin	SKLOIS, Chinese Academy of Sciences, China
Michael Locasto	Columbia University, USA
Masahiro MAMBO	Tsukuba University, Japan
Wenbo Mao	HP, Beijing, China
David Naccache	ENS, France
Rei Safavi-Naini	Calgary, Canada
Mridul Nandi	Indian Statistical Institute, India
Juan Gonzalez Nieto	QUT, Australia
Giuseppe Persiano	University of Salerno, Italy
Junji Shikata	University of Yokohama, Japan
Vitaly Shmatikov	University of Texas at Austin, USA
Francesco Sica	Mount Allison University, Canada
Rainer Steinwandt	Florida Atlantic University, USA
Willy Susilo	UWO, Australia
Bogdan Warinschi	University of Bristol, UK
DongHo Won	Sungkyunkwan University, Korea
Chuankun Wu	SKLOIS, Chinese Academy of Sciences, China
Shouhuai Xu	University of Texas at San Antonio, USA
Yongjin Yeom	NSRI, Korea
Yuefei Zhu	Information Engineering University, China

Organizing Committee Co-chairs

Dongdai LIN	SKLOIS, Chinese Academy of Sciences, China
Yanhui Niu	Qinhai University for Nationalities, China
Chuankun Wu	SKLOIS, Chinese Academy of Sciences, China

Organizing Committee

Jiwu Jing	SKLOIS, Chinese Academy of Sciences, China
Fuming Qi	Qinhai University for Nationalities, China
Shengfu Zhang	Qinhai University for Nationalities, China
Yuqing Zhang	SKLOIS, Chinese Academy of Sciences, China
Zhenfeng Zhang	SKLOIS, Chinese Academy of Sciences, China

Secretary and Treasurer

Yi Qin	SKLOIS, Chinese Academy of Sciences, China

WEB/Registration

Guangsheng Miao	SKLOIS, Chinese Academy of Sciences, China

Table of Contents

Invited Talks

Cryptanalysis of the SFLASH Signature Scheme (Extended Abstract) 1
Vivien Dubois, Pierre-Alain Fouque, Adi Shamir, and Jacques Stern

On the Evolution of User Authentication: Non-bilateral Factors 5
Moti Yung

Digital Signature Schemes

ECDSA-Verifiable Signcryption Scheme with Signature Verification on the Signcrypted Message 11
Raylin Tso, Takeshi Okamoto, and Eiji Okamoto

Provably Secure Identity-Based Undeniable Signatures with Selective and Universal Convertibility 25
Wei Wu, Yi Mu, Willy Susilo, and Xinyi Huang

An Efficient ID-Based Proxy Signature Scheme from Pairings 40
Chunxiang Gu and Yuefei Zhu

Block Cipher

Improved and Multiple Linear Cryptanalysis of Reduced Round Serpent 51
B. Collard, F.-X. Standaert, and J.-J. Quisquater

Linear Slide Attacks on the KeeLoq Block Cipher 66
Andrey Bogdanov

Key Management

A Key Predistribution Scheme Based on 3-Designs 81
Junwu Dong, Dingyi Pei, and Xueli Wang

Provably Secure N-Party Authenticated Key Exchange in the Multicast DPWA Setting 93
Weijia Wang, Lei Hu, and Yong Li

A Provably Secure One-Pass Two-Party Key Establishment Protocol . . . 108
K. Chalkias, S.T. Halkidis, D. Hristu-Varsakelis, G. Stephanides, and A. Alexiadis

Zero Knowledge and Secure Computation Protocols

Resettable Zero Knowledge with Concurrent Soundness in the Bare Public-Key Model under Standard Assumption 123
Yi Deng and Dongdai Lin

Secure Two-Party Computation of Squared Euclidean Distances in the Presence of Malicious Adversaries 138
Marc Mouffron, Frederic Rousseau, and Huafei Zhu

A Discrete-Logarithm Based Non-interactive Non-malleable Commitment Scheme with an Online Knowledge Extractor 153
Ning Ding and Dawu Gu

Secret Sharing

Verifiable Multi-secret Sharing Schemes for Multiple Threshold Access Structures 167
Christophe Tartary, Josef Pieprzyk, and Huaxiong Wang

Key Management Based on Hierarchical Secret Sharing in Ad-Hoc Networks 182
Chuangui Ma and Rui Cheng

Probabilistic (n, n) Visual Secret Sharing Scheme for Grayscale Images 192
Daoshun Wang, Xiaobo Li, and Feng Yi

Stream Cipher and Pseudorandomness

Mutually Clock-Controlled Feedback Shift Registers Provide Resistance to Algebraic Attacks 201
Sultan Al Hinai, Lynn Margaret Batten, and Bernard Colbert

Four Families of Binary Sequences with Low Correlation and Large Linear Complexity 216
Jin-Song Wang and Wen-Feng Qi

Pseudo-Randomness of Discrete-Log Sequences from Elliptic Curves 231
Zhixiong Chen, Ning Zhang, and Guozhen Xiao

Improved Bounds on the Linear Complexity of Keystreams Obtained by Filter Generators 246
Nicholas Kolokotronis, Konstantinos Limniotis, and Nicholas Kalouptsidis

Boolean Functions

Linear Equation on Polynomial Single Cycle T-Functions 256
Jin-Song Wang and Wen-Feng Qi

Weight Support Technique and the Symmetric Boolean Functions with Maximum Algebraic Immunity on Even Number of Variables 271
Longjiang Qu and Chao Li

Privacy and Deniability

Anonymity and k-Choice Identities 283
Jacek Cichoń and Mirosław Kutyłowski

Deniable Authentication on the Internet (Extended Abstract) 298
Shaoquan Jiang

Orthogonality between Key Privacy and Data Privacy, Revisited 313
Rui Zhang, Goichiro Hanaoka, and Hideki Imai

Unlinkable Randomizable Signature and Its Application in Group Signature 328
Sujing Zhou and Dongdai Lin

Hash Functions

An Improved Collision Attack on MD5 Algorithm 343
Shiwei Chen and Chenhui Jin

Multivariates Polynomials for Hashing 358
Jintai Ding and Bo-Yin Yang

Public Key Cryptosystems

Efficient Public Key Encryption with Keyword Search Schemes from Pairings 372
Chunxiang Gu, Yuefei Zhu, and Heng Pan

Multi-Identity Single-Key Decryption without Random Oracles 384
Fuchun Guo, Yi Mu, Zhide Chen, and Li Xu

Public Key Analysis

Kipnis-Shamir Attack on HFE Revisited 399
Xin Jiang, Jintai Ding, and Lei Hu

Cryptanalysis of General Lu-Lee Type Systems 412
Haijian Zhou, Ping Luo, Daoshun Wang, and Yiqi Dai

A Timing-Resistant Elliptic Curve Backdoor in RSA 427
Adam L. Young and Moti Yung

Application Security

A Watermarking Scheme in the Encrypted Domain for Watermarking Protocol 442
Bin Zhao, Lanjun Dang, Weidong Kou, Jun Zhang, Zan Li, and Kai Fan

Security Enhancement of a Flexible Payment Scheme and Its Role-Based Access Control 457
Chin-Chen Chang, Yi-Fang Cheng, and Iuon-Chang Lin

Systems Security and Trusted Computing

Building Trusted Sub-domain for the Grid with Trusted Computing 463
Jing Zhan, Huanguo Zhang, and Fei Yan

Enhanced Security by OS-Oriented Encapsulation in TPM-Enabled DRM 472
Yongdong Wu, Feng Bao, Robert H. Deng, Marc Mouffron, and Frederic Rousseau

Online Tracing Scanning Worm with Sliding Window 482
Yang Xiang and Qiang Li

Network Security

A New Proactive Defense Model Based on Intrusion Deception and Traceback 497
Junfeng Tian and Ning Li

On Modeling Post Decryption Error Processes in UMTS Air Interface 507
Fouz Sattar and Muid Mufti

A Simple, Smart and Extensible Framework for Network Security Measurement 517
Feng Cheng, Christian Wolter, and Christoph Meinel

Author Index 533