Information Security
and Cryptology

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

Feng Bao
Institute for Infocomm Research
1 Fusionopolis Way, #19-01 Conexus, 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

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.
springer.com
© Springer-Verlag Berlin Heidelberg 2010
Printed in Germany

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
VIII Organization

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

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integral Cryptanalysis of ARIA</td>
<td>1</td>
</tr>
<tr>
<td>Ping Li, Bing Sun, and Chao Li</td>
<td></td>
</tr>
<tr>
<td>Cryptanalysis of the ESSENCE Family of Hash Functions</td>
<td>15</td>
</tr>
<tr>
<td>Nicky Mouha, Gautham Sekar, Jean-Philippe Aumasson,</td>
<td></td>
</tr>
<tr>
<td>Thomas Peyrin, Søren S. Thomsen, Meltem Sönmez Turan, and</td>
<td></td>
</tr>
<tr>
<td>Bart Preneel</td>
<td></td>
</tr>
<tr>
<td>Differential-Multiple Linear Cryptanalysis</td>
<td>35</td>
</tr>
<tr>
<td>Zhiqiang Liu, Dawu Gu, Jing Zhang, and Wei Li</td>
<td></td>
</tr>
<tr>
<td>Differential Attack on Five Rounds of the SC2000 Block Cipher</td>
<td>50</td>
</tr>
<tr>
<td>Jiqiang Lu</td>
<td></td>
</tr>
</tbody>
</table>

## Signature and Signcryption

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pairing-Based Nominative Signatures with Selective and Universal</td>
<td>60</td>
</tr>
<tr>
<td>Convertibility</td>
<td></td>
</tr>
<tr>
<td>Wei Zhao and Dingfeng Ye</td>
<td></td>
</tr>
<tr>
<td>Cryptanalysis of Certificateless Signcryption Schemes and an Efficient</td>
<td>75</td>
</tr>
<tr>
<td>Construction without Pairing</td>
<td></td>
</tr>
<tr>
<td>S. Sharmila Deva Selvi, S. Sree Vivek, and C. Pandu Rangan</td>
<td></td>
</tr>
<tr>
<td>Sanitizable Signatures with Strong Transparency in the Standard Model</td>
<td>93</td>
</tr>
<tr>
<td>Shivank Agrawal, Swarun Kumar, Amjed Shareef, and C. Pandu Rangan</td>
<td></td>
</tr>
<tr>
<td>Breaking and Building of Threshold Signcryption Schemes</td>
<td>108</td>
</tr>
<tr>
<td>S. Sharmila Deva Selvi, S. Sree Vivek, Shilpi Noyak, and</td>
<td></td>
</tr>
<tr>
<td>C. Pandu Rangan</td>
<td></td>
</tr>
</tbody>
</table>

## Key Exchange

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provably Secure Password-Authenticated Group Key Exchange with</td>
<td>124</td>
</tr>
<tr>
<td>Different Passwords under Standard Assumption</td>
<td></td>
</tr>
<tr>
<td>Fengjiao Wang and Yuqing Zhang</td>
<td></td>
</tr>
<tr>
<td>An Enhanced Password Authenticated Key Agreement Protocol for</td>
<td>134</td>
</tr>
<tr>
<td>Wireless Mobile Network</td>
<td></td>
</tr>
<tr>
<td>Zhigang Gao and Dengguo Feng</td>
<td></td>
</tr>
</tbody>
</table>
Efficient Password-Based Authenticated Key Exchange Protocol in the UC Framework .................................................. 144  
Xuexian Hu and Wenfen Liu

Private Computations

Efficient Generalized Selective Private Function Evaluation with Applications in Biometric Authentication .................. 154  
Helger Lipmaa and Bingsheng Zhang

Optionally Identifiable Private Handshakes ............................................. 164  
Yanjiang Yang, Jian Weng, Jianying Zhou, and Ying Qiu

Communication Efficient Statistical Asynchronous Multiparty Computation with Optimal Resilience ......................... 179  
Arpita Patra, Ashish Choudhury, and C. Pandu Rangan

Cipher Design and Analysis

Gemstone: A New Stream Cipher Using Coupled Map Lattice .......... 198  
Ruming Yin, Jian Yuan, Qiuhua Yang, Xiuming Shan, and Xiqin Wang

Proposition of Two Cipher Structures .................................................. 215  
Lei Zhang, Wenling Wu, and Liting Zhang

Hardware Framework for the Rabbit Stream Cipher ......................... 230  
Deian Stefan

Linearity within the SMS4 Block Cipher .............................................. 248  
Muhammad Reza Z’aba, Leonie Simpson, Ed Dawson, and Kenneth Wong

Algebraic Cryptanalysis of Curry and Flurry Using Correlated Messages ............................................................ 266  
Jean-Charles Faugère and Ludovic Perret

Public Key Cryptography

Weak Keys in RSA with Primes Sharing Least Significant Bits .......... 278  
Xianmeng Meng and Jingguo Bi

Hybrid Proxy Re-encryption Scheme for Attribute-Based Encryption ... 288  
Takeo Mizuno and Hiroshi Doi

Constructing Better KEMs with Partial Message Recovery ............. 303  
Rui Zhang and Hideki Imai
Network and System Security

A Novel Contagion-Like Patch Dissemination Mechanism against Peer-to-Peer File-Sharing Worms ................................................. 313
Xiaofeng Nie, Jiwu Jing, and Yuewu Wang

Remodeling Vulnerability Information ........................................... 324
Feng Cheng, Sebastian Roschke, Robert Schuppenies, and Christoph Meinel

Using Strategy Objectives for Network Security Analysis ............... 337
Elie Bursztein and John C. Mitchell

Hardware Security

A DAA Scheme Requiring Less TPM Resources ............................ 350
Liqun Chen

Full-Custom VLSI Design of a Unified Multiplier for Elliptic Curve Cryptography on RFID Tags .......................................................... 366
Johann Großschädl

Weaknesses in Two Recent Lightweight RFID Authentication Protocols ............................................................................. 383
Pedro Peris-Lopez, Julio C. Hernandez-Castro, Juan M.E. Tapiador, Tieyan Li, and Jan C.A. van der Lubbe

Algebraic Side-Channel Attacks ...................................................... 393
Mathieu Renauld and François-Xavier Standaert

Web Security

CAPTCHA Phishing: A Practical Attack on Human Interaction Proofing ................................................................................... 411
Le Kang and Ji Xiang

An Attack and Repair of Secure Web Transaction Protocol for Anonymous Mobile Agents ....................................................... 426
Saba Jalal and Brian King

A Formal Language for Specifying Complex XML Authorisations with Temporal Constraints .................................. 443
Sean Policarpio and Yan Zhang

Author Index ............................................................................ 459