# Lecture Notes in Computer Science 6980

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

## Editorial Board

David Hutchison
*Lancaster University, UK*

Takeo Kanade
*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler
*University of Surrey, Guildford, UK*

Jon M. Kleinberg
*Cornell University, Ithaca, NY, USA*

Alfred Kobsa
*University of California, Irvine, CA, USA*

Friedemann Mattern
*ETH Zurich, Switzerland*

John C. Mitchell
*Stanford University, CA, USA*

Moni Naor
*Weizmann Institute of Science, Rehovot, Israel*

Oscar Nierstrasz
*University of Bern, Switzerland*

C. Pandu Rangan
*Indian Institute of Technology, Madras, India*

Bernhard Steffen
*TU Dortmund University, Germany*

Madhu Sudan
*Microsoft Research, Cambridge, MA, USA*

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*

Xavier Boyen  Xiaofeng Chen (Eds.)

# Provable Security

5th International Conference, ProvSec 2011
Xi'an, China, October 16-18, 2011
Proceedings

Springer

Volume Editors

Xavier Boyen
Palo Alto Research Center
Palo Alto, CA 94304, USA
E-mail: xb@boyen.org

Xiaofeng Chen
Xidian University
School of Telecommunications Engineering
Xi'an, 710071, China
E-mail: xfchen@xidian.edu.cn

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-24315-8 e-ISBN 978-3-642-24316-5
DOI 10.1007/978-3-642-24316-5
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011936538

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

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2011

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.
The use of general descriptive names, registered names, trademarks, 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.

*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 Fifth International Conference on Provable Security (ProvSec 2011) was held in Xi'an, China, October 16–18, 2011. This volume contains papers that were accepted to the academic track of the conference. The Program Committee also invited two distinguished researchers to deliver their keynote talks. The first speaker was Jens Groth from University College London, UK. His talk was entitled "Optimal Structure-Preserving Signatures." The second speaker was Vipul Goyal from Microsoft Research, India. His talk was entitled "Secure Composition of Cryptographic Protocols."

The conference received 75 submissions this year. Each paper was assigned to four referees and we tried our best to ensure that each paper received a thorough and fair review. We are indebted to the members of the Program Committee and the external reviewers for all their hard work. The committee accepted 22 regular papers and 4 short papers to be included in the conference program. These proceedings contain revised versions of the accepted papers. While revisions are expected to take the referees' comments into account, this was not enforced and the authors bear full responsibility for the content of their papers.

In addition to the academic track, the conference hosted a non-archival technical track whose papers were also carefully selected from among the submissions.

It is our pleasure to thank the General Chair Hui Li, the Publicity Co-chairs Qingqi Pei and Yueyu Zhang, and the Chair of the Organizing Committee Weiyi Yin for their great help and support in putting this conference together. We also appreciate the developer of the EasyChair conference system which we used for this conference. Special thanks for Ilsun You and Fatos Xhafa for their great support. Finally, we are grateful to the National Natural Science Foundation of China (NSFC), Key Laboratory of Computer Networks and Information Security, Ministry of Education, Xidian University for sponsoring the conference.

October 2011

Xavier Boyen
Xiaofeng Chen

# ProvSec 2011

# 5th International Conference on Provable Security

October 16–18, Xi'an, China

*Sponsored by*
The National Natural Science Foundation of China (NSFC)
Key Laboratory of Computer Networks and Information Security,
Ministry of Education, Xidian University, China

## General Chair

| | |
|---|---|
| Hui Li | Xidian University, China |

## Program Co-chairs

| | |
|---|---|
| Xavier Boyen | PARC, USA |
| Xiaofeng Chen | Xidian University, China |

## Program Committee

| | |
|---|---|
| Joonsang Baek | KUSTAR, UAE |
| Feng Bao | Institute for Infocomm Research, Singapore |
| Dario Catalano | Università di Catania, Italy |
| Kefei Chen | Shanghai Jiaotong University, China |
| Liqun Chen | Hewlett-Packard Laboratories, UK |
| Sherman S.M. Chow | University of Waterloo, Canada |
| Dengguo Feng | Chinese Academy of Sciences, China |
| Marc Fischlin | Darmstadt University of Technology, Germany |
| Matthew Green | The Johns Hopkins University, USA |
| Yupu Hu | Xidian University, China |
| Xinyi Huang | Institute for Infocomm Research, Singapore |
| Kwangjo Kim | KAIST, Korea |
| Noboru Kunihiro | University of Tokyo, Japan |
| Kaoru Kurosawa | Ibaraki University, Japan |
| Fabien Laguillaumie | University of Caen, France |
| Jin Li | Guangzhou University, China |
| Benoit Libert | Université Catholique de Louvain, Belgium |
| Jianfeng Ma | Xidian University, China |
| Wojciech Mazurczyk | Warsaw University of Technology, Poland |
| Yi Mu | University of Wollongong, Australia |

| | |
|---|---|
| David Naccache | École normale supérieure, France |
| Claudio Orlandi | Bar Ilan University, Israel |
| Olivier Pereira | UCL, Belgium |
| Josef Pieprzyk | Macquarie University, Australia |
| Kouichi Sakurai | Kyushu University, Japan |
| Palash Sarkar | Indian Statistical Institute, India |
| Alice Silverberg | University of California, Irvine, USA |
| Ron Steinfeld | Macquarie University, Australia |
| Willy Susilo | University of Wollongong, Australia |
| Tsuyoshi Takagi | Future University-Hakodate, Japan |
| Damien Vergnaud | École normale supérieure, France |
| Huaxiong Wang | Nanyang Technological University, Singapore |
| Duncan Wong | City University of Hong Kong, China |
| Qianhong Wu | Universitat Rovira i Virgili, Spain |
| Shouhuai Xu | University of Texas at San Antonio, USA |
| Bo Yang | South China Agricultural University, China |
| Ilsun You | Korean Bible University, Korea |
| Fangguo Zhang | Sun Yan-Sen Univeristy, China |
| Rui Zhang | Tokyo University of Science, Japan |
| Yunlei Zhao | Fudan University, China |
| Yuliang Zheng | University of North Carolina at Charlotte, USA |
| Jianying Zhou | Institute for Infocomm Research, Singapore |

## Steering Committee

| | |
|---|---|
| Feng Bao | Institute for Infocomm Research, Singapore |
| Xavier Boyen | PARC, USA |
| Yi Mu | University of Wollongong, Australia |
| Josef Pieprzyk | Macquarie University, Australia |
| Willy Susilo | University of Wollongong, Australia |

## Publicity Co-chairs

| | |
|---|---|
| Qingqi Pei | Xidian University, China |
| Yueyu Zhang | Xidian University, China |

## Organizing Committee

| | |
|---|---|
| Weiyi Yin | Xidian University, China |
| Yuanyuan Zuo | Xidian University, China |
| Fengrong Zhang | Xidian University, China |
| Yinghui Zhang | Xidian University, China |

## External Reviewers

Au, Man Ho
Bhattacharyya, Rishiraj
Brzuska, Christina
Canard, Sébastien
Castagnos, Guilhem
Chang, Donghoon
Chatterjee, Sanjit
Chen, Jie
Chen, Yu
Choudhury, Ashish
Chu, Cheng-Kang
Dagdelen, Özgür
Deng, Yi
Di Raimondo, Mario
Fan, Jia
Fiore, Dario
Furukawa, Jun
Gao, Wei
Guo, Fuchun
Han, Jinguang
Hanaoka, Goichiro
Hanatani, Yoshikazu
Herranz, Javier
Hirose, Shoichi
Iwata, Tetsu
Kawai, Yutaka
Keller, Marcel
Lai, Junzuo
Li, Fagen
Li, Ximing
Liu, Joseph
Long, Yu
Lv, Xixiang
Ma, Sha
Ma, Xu
Mandell Freeman, David
Mao, Xianping
Matsuda, Takahiro
Mawet, Sophie
Meiklejohn, Sarah
Meldgaard, Sigurd
Mitsunari, Shigeo
Naito, Yusuke
Nandi, Mridul
Nishide, Takashi
Nordholdt, Peter
Ogata, Wakaha
Onete, Maria Cristina
Orumiehchiha, Ali Mohammad
Pan, Jiaxin
Pandey, Omkant
Pastro, Valerio
Pehlivanoglu, Serdar
Peng, Kun
Peters, Thomas
Phong, Le Trieu
Qian, Haifeng
Qin, Bo
Wang, Qinglong
Ramanna, Somindu
Schroeder, Dominique
Sen Gupta, Sourav
Jiang, Shaoquan
Singh, Shashank
Steine, Asgeir
Su, Chunhua
Sun, Weiwei
Sur, Chul
Tan, Xiao
Teranishi, Isamu
Visconti, Ivan
Wan, Junzhou
Wan, Yanchun
Wang, Liangliang
Wang, Ping
Wang, Yongtao
Weng, Jian
Wu, Wei
Wu, Yongdong
Xu, Lingling
Yamada, Shota
Yang, Dexin
Yang, Yanjiang
Yoneyama, Kazuki
Yu, Yong
Zhang, Lei
Zhang, Liangfeng
Zhang, Mingwu
Zhang, Yun
Zhang, Zongyang
Zhao, Xingwen
Zheng, Qingji
Zhu, Huafei

# Table of Contents

## Invited Talks

Optimal Structure-Preserving Signatures . . . . . 1
*Jens Groth*

Secure Composition of Cryptographic Protocols . . . . . 2
*Vipul Goyal*

## Cryptographic Primitives

Secure Two-Party Computation over a Z-Channel . . . . . 3
*Paolo Palmieri and Olivier Pereira*

Precise Time and Space Simulatable Zero-Knowledge . . . . . 16
*Ning Ding and Dawu Gu*

Weak Oblivious Transfer from Strong One-Way Functions . . . . . 34
*Keisuke Tanaka, Akihiro Yamada, and Kenji Yasunaga*

Simulatable Adaptive Oblivious Transfer with Statistical Receiver's Privacy . . . . . 52
*Bingsheng Zhang*

## Encryption

Verifiable Security of Boneh-Franklin Identity-Based Encryption . . . . . 68
*Gilles Barthe, Federico Olmedo, and Santiago Zanella Béguelin*

Efficient Ciphertext Policy Attribute-Based Encryption with Constant-Size Ciphertext and Constant Computation-Cost . . . . . 84
*Cheng Chen, Zhenfeng Zhang, and Dengguo Feng*

Fully Distributed Broadcast Encryption . . . . . 102
*Qianhong Wu, Bo Qin, Lei Zhang, and Josep Domingo-Ferrer*

Efficient Identity-Based Signcryption in the Standard Model . . . . . 120
*Fagen Li, Fahad Bin Muhaya, Mingwu Zhang, and Tsuyoshi Takagi*

Toward Compact Public Key Encryption Based on CDH Assumption via Extended Twin DH Assumption . . . . . 138
*Yoshikazu Hanatani, Hirofumi Muratani, and Tomoko Yonemura*

Anonymous Encryption with Partial-Order Subset Delegation Functionality . . . . . 154
*Mingwu Zhang, Takashi Nishide, Bo Yang, and Tsuyoshi Takagi*

## Cryptographic Protocols

Concurrent Signatures with Fully Negotiable Binding Control . . . . . 170
*Tsz Hon Yuen, Duncan S. Wong, Willy Susilo, and Qiong Huang*

Secure Obfuscation of Encrypted Verifiable Encrypted Signatures . . . . . 188
*Rong Cheng, Bo Zhang, and Fangguo Zhang*

Identity-Based Trace and Revoke Schemes . . . . . 204
*Duong Hieu Phan and Viet Cuong Trinh*

Universally Composable Private Proximity Testing . . . . . 222
*Rafael Tonicelli, Bernardo Machado David, and Vinícius de Morais Alves*

Generic Constant-Round Oblivious Sorting Algorithm for MPC . . . . . 240
*Bingsheng Zhang*

General Construction of Chameleon All-But-One Trapdoor Functions . . . 257
*Shengli Liu, Junzuo Lai, and Robert H. Deng*

## Security Models and Framework

PolyE+CTR: A Swiss-Army-Knife Mode for Block Ciphers . . . . . 266
*Liting Zhang, Wenling Wu, and Peng Wang*

Security of Practical Cryptosystems Using Merkle-Damgård Hash Function in the Ideal Cipher Model . . . . . 281
*Yusuke Naito, Kazuki Yoneyama, Lei Wang, and Kazuo Ohta*

Key-Dependent Message Security for Division Function: Discouraging Anonymous Credential Sharing . . . . . 297
*Xianhui Lu, Bao Li, Qixiang Mei, and Haixia Xu*

Randomness Leakage in the KEM/DEM Framework . . . . . 309
*Hitoshi Namiki, Keisuke Tanaka, and Kenji Yasunaga*

Generalized Learning Problems and Applications to Non-commutative Cryptography (Extended Abstract) . . . . . 324
*Gilbert Baumslag, Nelly Fazio, Antonio R. Nicolosi, Vladimir Shpilrain, and William E. Skeith III*

A Novel Framework for Protocol Analysis . . . . . 340
*Kristian Gjøsteen, George Petrides, and Asgeir Steine*

## Key Agreement

Taxonomical Security Consideration of Authenticated Key Exchange Resilient to Intermediate Computation Leakage . . . . . 348
*Kazuki Yoneyama and Yunlei Zhao*

Gateway-Oriented Password-Authenticated Key Exchange Protocol with Stronger Security . . . . . 366
*Fushan Wei, Chuangui Ma, and Zhenfeng Zhang*

TMQV: A Strongly eCK-Secure Diffie-Hellman Protocol without Gap Assumption . . . . . 380
*Jiaxin Pan and Libin Wang*

Strongly Secure One Round Authenticated Key Exchange Protocol with Perfect Forward Security . . . . . 389
*Hai Huang*

**Author Index** . . . . . 399