

*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*

Tsuyoshi Takagi Guilin Wang  
Zhiguang Qin Shaoquan Jiang Yong Yu (Eds.)

# Provable Security

6th International Conference, ProvSec 2012  
Chengdu, China, September 26-28, 2012  
Proceedings

## Volume Editors

Tsuyoshi Takagi  
Kyushu University  
Institute of Mathematics for Industry  
744, Motooka, Nishi-ku, Fukuoka 819-0395, Japan  
E-mail: takagi@imi.kyushu-u.ac.jp

Guilin Wang  
University of Wollongong  
School of Computer Science and Software Engineering  
Northfields Avenue, Wollongong NSW 2522, Australia  
E-mail: guilin@uow.edu.au

Zhiguang Qin  
Shaoquan Jiang  
Yong Yu  
University of Electronic Science and Technology of China  
School of Computer Science and Engineering  
2006 Xiyuan Rd, HighTech West, Chengdu, 611731, China  
E-mail: {qinzg, yuyong}@uestc.edu.cn, shaoquan.jiang@gmail.com

ISSN 0302-9743 e-ISSN 1611-3349  
ISBN 978-3-642-33271-5 e-ISBN 978-3-642-33272-2  
DOI 10.1007/978-3-642-33272-2  
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012946106

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

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2012

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 6th International Conference on Provable Security (ProvSec 2012) was held in Chengdu, China, September 26–28, 2012. The workshop was organized by the University of Electronic Science and Technology of China.

ProvSec 2012 received 66 submissions from 15 different countries all over the world. The review process was a challenging task. Almost all submissions were carefully evaluated by four reviewers for a total of 262 reviews, and then discussed among the Program Committee. Moreover, 62 external subreviewers gave review comments on their area of expertise. The Program Committee selected 20 papers for the program out of 66 submissions. Among these 20 papers, 16 were accepted as full papers and four as short papers. Further, the program featured two excellent invited talks given by Masayuki Abe (Secure Platform Laboratories, NTT Corporation, Japan) titled “Tools over Bilinear Groups for Modular Design of Cryptographic Tasks” and Victor Shoup (New York University, USA) titled “GNUC Is not UC.”

Many people contributed to the success of ProvSec 2012. First we would like to thank all of the authors for submitting their works. We deeply thank the 46 Program Committee members as well as the external reviewers for their volunteer work of reading and discussing the submissions. We thank the Publicity and Publication Co-chairs, Shaoquan Jiang and Yong Yu, for their support. We also would like to thank the local Organizing Committee, Yongjian Liao, Chunxiang Xu, Sheng Cao, and Xuyun Nie, for their dedication and commitment in organizing the conference. Finally, we want to express our gratitude to our generous sponsor: the University of Electronic Science and Technology of China.

September 2012

Tsuyoshi Takagi  
Guilin Wang

# ProvSec 2012

The 6th International Conference on Provable Security

Chengdu, China

September 26–28, 2012

*Organized and Sponsored by the University of Electronic Science and  
Technology of China (UESTC)*

## General Chair

Zhiguang Qin

UESTC, China

## Publication and Publicity Co-chairs

Shaoquan Jiang

UESTC, China

Yong Yu

UESTC, China

## Program Co-chairs

Tsuyoshi Takagi

Kyushu University, Japan

Guilin Wang

University of Wollongong, Australia

## Program Committee

Michel Abdalla

ENS and CNRS, France

Man Ho Au

University of Wollongong, Australia

Feng Bao

Institute for Infocomm Research, Singapore

Carlo Blundo

University of Salerno, Italy

Zhenfu Cao

Shanghai Jiaotong University, China

Liqun Chen

Hewlett-Packard Labs, Bristol, UK

Xiaofeng Chen

Xidian University, China

Raymond Choo

University of South Australia, Australia

Georg Fuchsbaauer

University of Bristol, UK

David Galindo

University of Luxembourg, Luxembourg

Wei Gao

Ludong University, China

Goichiro Hanaoka

AIST, Japan

Mingxing He

Xihua University, China

Swee-Huay Heng

Multimedia University, Malaysia

Javier Herranz

Universitat Politècnica de Catalunya, Spain

Qiong Huang

South China Agricultural University, China

Tetsu Iwata

Nagoya University, Japan

Shaoquan Jiang	UESTC, China
Aggelos Kiayias	University of Connecticut, USA
Kaoru Kurosawa	Ibaraki University, Japan
Fagen Li	UESTC, China
Benoit Libert	Université Catholique de Louvain, Belgium
Joseph K. Liu	Institute for Infocomm Research, Singapore
Mark Manulis	TU Darmstadt, Germany
Kanta Matsuura	University of Tokyo, Japan
Atsuko Miyaji	JAIST, Japan
Joern Mueller-Quade	Karlsruhe Institute of Technology, Germany
David Naccache	École Normale Supérieure, France
Juan Manuel González Nieto	QUT, Australia
Claudio Orlandi	Bar Ilan University, Israel
Raphael C.-W. Phan	Loughborough University, UK
Josef Pieprzyk	Macquarie University, Australia
C. Pandu Rangan	IIT Madras, India
M. R. Reyhanitabar	University of Wollongong, Australia
Palash Sarkar	Indian Statistical Institute, India
Willy Susilo	University of Wollongong, Australia
Katsuyuki Takashima	Mitsubishi Electric, Japan
Keisuke Tanaka	Tokyo Institute of Technology, Japan
Mehdi Tibouchi	NTT, Japan
Wen-Guey Tzeng	National Chiao Tung University, Taiwan
Huaxiong Wang	NTU, Singapore
Duncan S. Wong	City University of Hong Kong, China
Rui Xue	Chinese Academy of Sciences, China
Alec Yasinsac	University of South Alabama, USA
Yong Yu	UESTC, China
Fanguo Zhang	Sun Yat-sen University, China
Mingwu Zhang	South China Agricultural University, China
Yuliang Zheng	UNC at Charlotte, USA

## External Reviewers

Elena Andreeva	Angelo De Caro	Zhen Liu
Toshinori Araki	Emiliano De Cristofaro	Jacob Loftus
George Argyros	Yi Deng	Xu Ma
Rouzbeh Behnia	Nico Doettling	Cuauhtemoc
Jie Chen	Keita Emura	Mancillas-Lopez
Zhenhua Chen	Vincent Grosso	Ben Martini
Zhili Chen	Fuchun Guo	Takahiro Matsuda
Kai Yuen Cheong	Vincenzo Iovino	Shigeo Mitsunari
Ji-Jian Chin	Jin Li	Khoa Nguyen
Cas Cremers	Ximing Li	Ryo Nishimaki
Gareth Davies	Kaitai Liang	Ryo Nojima

Kazumasa Omote  
Serdar Pehlivanoglu  
Thomas Peters  
Le Trieu Phong  
Somindu Ramanna  
Yusuke Sakai  
Katerina Samari  
Jacob Schuldt  
Sharmila Deva Selvi  
Ying Sun

Syh-Yuan Tan  
Xiao Tan  
Qiang Tang  
Yiannis Tselekounis  
Sree Vivek  
Jianfeng Wang  
Keita Xagawa  
Li Xiao  
Xiang Xie  
Shota Yamada

Naoto Yanai  
Xu Shi You  
Qingyi Zeng  
Shengke Zeng  
Bo Zhang  
Jinshuang Zhang  
Liangfeng Zhang  
Rui Zhang  
Yinghui Zhang  
Yun Zhang

# Table of Contents

## Invited Talk

Tools over Bilinear Groups for Modular Design of Cryptographic Tasks.....	1
<i>Masayuki Abe</i>	

## Signature Schemes

One-Move Convertible Nominative Signature in the Standard Model....	2
<i>Dennis Y.W. Liu and Duncan S. Wong</i>	
Efficient and Random Oracle-Free Conditionally Anonymous Ring Signature .....	21
<i>Shengke Zeng, Zhiguang Qin, Qing Lu, and Qinyi Li</i>	
ID Based Signcryption Scheme in Standard Model .....	35
<i>S. Sharmila Deva Selvi, S. Sree Vivek, Dhinakaran Vinayagamurthy, and C. Pandu Rangan</i>	
Combined Public-Key Schemes: The Case of ABE and ABS .....	53
<i>Cheng Chen, Jie Chen, Hoon Wei Lim, Zhenfeng Zhang, and Dengguo Feng</i>	

## Foundations

Several Weak Bit-Commitments Using Seal-Once Tamper-Evident Devices .....	70
<i>Ioana Boureanu and Serge Vaudenay</i>	
Deterministic Random Oracles.....	88
<i>Margus Nütsoo</i>	
On the (Non-)Equivalence of UC Security Notions .....	104
<i>Oana Ciobotaru</i>	

## Leakage Resilience and Key Escrow

LR-UESDE: A Continual-Leakage Resilient Encryption with Unbounded Extensible Set Delegation .....	125
<i>Bo Yang and Mingwu Zhang</i>	



Anonymous Identity-Based Hash Proof System and Its Applications . . . .	143
<i>Yu Chen, Zongyang Zhang, Dongdai Lin, and Zhenfu Cao</i>	
Efficient Escrow-Free Identity-Based Signature . . . . .	161
<i>Yunmei Zhang, Joseph K. Liu, Xinyi Huang, Man Ho Au, and Willy Susilo</i>	

## Encryption Schemes

Perfect Keyword Privacy in PEKS Systems . . . . .	175
<i>Mototsugu Nishioka</i>	
Efficient Fully Secure Attribute-Based Encryption Schemes for General Access Structures . . . . .	193
<i>Tapas Pandit and Rana Barua</i>	
Symmetric Inner-Product Predicate Encryption Based on Three Groups . . . . .	215
<i>Masayuki Yoshino, Noboru Kunihiro, Ken Naganuma, and Hisayoshi Sato</i>	
Secure Keyword Search Using Bloom Filter with Specified Character Positions . . . . .	235
<i>Takanori Suga, Takashi Nishide, and Kouichi Sakurai</i>	

## Short Papers

Fully Secure Doubly-Spatial Encryption under Simple Assumptions . . . .	253
<i>Cheng Chen, Zhenfeng Zhang, and Dengguo Feng</i>	
Strongly Authenticated Key Exchange Protocol from Bilinear Groups without Random Oracles . . . . .	264
<i>Zheng Yang and Jörg Schwenk</i>	
Authenticated Key Exchange with Entities from Different Settings and Varied Groups . . . . .	276
<i>Yanfei Guo and Zhenfeng Zhang</i>	
On Capabilities of Hash Domain Extenders to Preserve Enhanced Security Properties . . . . .	288
<i>Mohammad Reza Reyhanitabar and Willy Susilo</i>	

**Information Theoretical Security**

Revisiting a Secret Sharing Approach to Network Codes ..... 300  
    *Zhaohui Tang, Hoon Wei Lim, and Huaxiong Wang*

Codes Based Tracing and Revoking Scheme with Constant  
Ciphertext ..... 318  
    *Xingwen Zhao and Hui Li*

**Author Index** ..... 337