

*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*

Mark D. Ryan Ben Smyth Guilin Wang (Eds.)

# Information Security Practice and Experience

8th International Conference, ISPEC 2012  
Hangzhou, China, April 9-12, 2012  
Proceedings

## Volume Editors

Mark D. Ryan  
University of Birmingham  
School of Computer Science  
Birmingham B15 2TT, UK  
E-mail: mdr@cs.bham.ac.uk

Ben Smyth  
Toshiba Corporation  
1, Komukai-Toshiba-Cho, Saiwai-ku  
Kawasaki 212-8582, Japan  
E-mail: toshiba@bensmyth.com

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

ISSN 0302-9743 e-ISSN 1611-3349  
ISBN 978-3-642-29100-5 e-ISBN 978-3-642-29101-2  
DOI 10.1007/978-3-642-29101-2  
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: Applied for

CR Subject Classification (1998): E.3, D.4.6, C.2.0, H.2.0, K.6.5, K.4.4, J.1

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 8th International Conference on Information Security Practice and Experience (ISPEC 2012) was hosted by Hangzhou Normal University in Hangzhou, China, between 9–12 April 2012.

The ISPEC conference series is an established forum that brings together researchers and practitioners to provide a confluence of new information security technologies, including their applications and their integration with IT systems in various vertical sectors. In previous years, ISPEC has taken place in Singapore (2005), Hangzhou, China (2006), Hong Kong, China (2007), Sydney, Australia (2008), Xi'an, China (2009), Seoul, Korea (2010), and Guangzhou, China (2011). For all sessions, as this one, the conference proceedings were published by Springer in the *Lecture Notes in Computer Science* series.

In total, 109 papers from 20 countries were submitted to ISPEC 2012, and 27 were selected for inclusion in the proceedings (acceptance rate 25%), including 20 full papers and 7 works-in-progress. The accepted papers cover multiple topics of information security and applied cryptography. Each submission was anonymously reviewed by at least three reviewers and the majority of papers were reviewed by four reviewers. We are grateful to the Program Committee, which was composed of more than 53 well-known security experts from 16 countries; we heartily thank them as well as all external reviewers for their time and valued contributions to the tough and time-consuming reviewing process. In addition to the paper presentations, the program also featured three invited talks and we are grateful to each speaker for accepting our invitation to participate in the conference.

There are many people who contributed to the success of ISPEC 2012. We sincerely thank the Honorary Chair, Xiuyuan Yu, and the General Chairs, Robert H. Deng and Qi Xie, for their strong support. We also thank the Organizing Committee – namely, Xiumei Li, Wenhao Liu, Shengbao Wang, Xianqin Xiang, Mingrui Yu, and Zhenming Yuan – for dealing with local issues. We are grateful to the authors from around the world for submitting and presenting their papers. We are also deeply grateful to the Program Committee members for their fair review. It would have been impossible to organize ISPEC 2012 without the hard work of all our chairs and committees. Finally, we would like to thank all the participants for their contribution to ISPEC 2012.

April 2012

Mark D. Ryan  
Ben Smyth  
Guilin Wang

# ISPEC 2012

## 8th International Conference on Information Security Practice and Experience

Hangzhou, China  
April 9–12, 2012

*Hosted by*

Hangzhou Normal University, China

### Honorary Chair

Xiuyuan Yu

Hangzhou Normal University, China

### General Chairs

Robert H. Deng  
Qi Xie

Singapore Management University, Singapore  
Hangzhou Normal University, China

### Program Chairs

Mark D. Ryan  
Guilin Wang

University of Birmingham, UK  
University of Wollongong, Australia

### Program Committee

Moritz Becker

Microsoft, Cambridge, UK

Sergiu Bursuc

University of Birmingham, UK

Rohit Chadha

ENS Cachan, France

David Chadwick

University of Kent, UK

Kostas Chatzikokolakis

École Polytechnique, France

Kefei Chen

Shanghai Jiaotong University, China

Tom Chothia

University of Birmingham, UK

Sherman S.M. Chow

University of Waterloo, Canada

Richard Clayton

University of Cambridge, UK

Jason Crampton

Royal Holloway, University of London, UK

Cas Cremers

ETH Zürich, Switzerland

Stéphanie Delaune

ENS Cachan, France

Xuhua Ding

Singapore Management University, Singapore

Pooya Farshim

TU Darmstadt, Germany

Flavio D. Garcia

Radboud University Nijmegen,  
The Netherlands

Dawu Gu	Shanghai Jiaotong University, China
Gerhard Hancke	Royal Holloway, University of London, UK
James Heather	University of Surrey, UK
Matt Henricksen	Institute for Infocomm Research, Singapore
Dalia Khader	University of Luxembourg, Luxembourg
Boris Köpf	IMDEA Software Institute, Spain
Steve Kremer	INRIA Nancy, France
Tieyan Li	Irdeto (Cloakware), China
Dongdai Lin	Chinese Academy of Science, China
Peng Liu	Pennsylvania State University, USA
Subhamoy Maitra	Indian Statistical Institute, India
Andrew Martin	University of Oxford, UK
Kanta Matsuura	University of Tokyo, Japan
Atsuko Miyaji	Japan Advanced Institute of Science and Technology, Japan
Sebastian Mödersheim	DTU Informatics, Denmark
Yi Mu	University of Wollongong, Australia
Shishir Nagaraja	IIIT Delhi, India
Eiji Okamoto	University of Tsukuba, Japan
Alfredo Pironti	INRIA, France
Saša Radomirović	Université du Luxembourg, Luxembourg
Douglas S. Reeves	North Carolina State University, USA
Kouichi Sakurai	Kyushu University, Japan
Ben Smyth	Toshiba Corporation, Japan
Sriramkrishnan Srinivasan	University of Surrey, UK
Tomasz Truderung	University of Trier, Germany
Bogdan Warinschi	University of Bristol, UK
Jian Weng	Jinan University, China
Duncan S. Wong	City University of Hong Kong, China
Yongdong Wu	Institute for Infocomm Research, Singapore
Yang Xiang	Deakin University, Australia
Jeff Yan	Newcastle University, UK
Danfeng Yao	Virginia Tech, USA
Sung-Ming Yen	National Central University, Taiwan
Hongbo Yu	Tsinghua University, China
Yong Yu	University of Electronic Science and Technology of China, China
Zhenfeng Zhang	Chinese Academy of Science, China
Yunlei Zhao	Fudan University, China
Jianying Zhou	Institute for Infocomm Research, Singapore

## Publication Chair

Ben Smyth	Toshiba Corporation, Japan
-----------	----------------------------

## Organizing Committee

Xiumei Li	Hangzhou Normal University, China
Wenhao Liu	Hangzhou Normal University, China
Shengbao Wang	Hangzhou Normal University, China
Xianqin Xiang	Hangzhou Normal University, China
Mingrui Yu	Hangzhou Normal University, China
Zhenming Yuan	Hangzhou Normal University, China

## External Reviewers

Shweta Agrawal	Satoshi Hada
Toru Akishita	Jinguang Han
Man Ho Au	Feng Hao
Matteo Avalu	Julio Cesar Hernandez-Castro
Joonsang Baek	Dennis Hofheinz
Subhadeep Banik	Xinyi Huang
Gilles Barthe	Sorina Ionica
Rana Barua	Vincenzo Iovino
Joseph Bonneau	Mahavir Jhavar
Sébastien Canard	Dingding Jia
Silvio Cesare	Jonathan Katz
Shan Chen	Wei Ming Khoo
Yu Chen	Markulf Kohlweiss
Kai-Yuen Cheong	Yuichi Komano
Céline Chevalier	Fabien Laguillaumie
Cheng-Kang Chu	Junzuo Lai
Ozgur Dagdelen	Jean Lancrenon
George Danezis	Fagen Li
Prem Laxman Das	Juanru Li
Angelo De Caro	Zhenqi Li
Gerhard De Koning Gans	Hongliang Liang
Ning Ding	Kaitai Liang
Ehab Elsalamouny	Changlu Lin
Jia Fan	Hsi-Chung Lin
Daniel Fett	Joseph Liu
Pierre-Alain Fouque	Yamin Liu
Steven Galbraith	Zhen Liu
David Galindo	Zhiqiang Liu
Sugata Gangopadhyay	Zongbin Liu
Wei Gao	Yu Long
Thomas Gross	Haining Lu
Haihua Gu	Jiqiang Lu
Hauhua Gu	Xianhui Lu
Fuchun Guo	Jiqiang Lv

Sergio Maffei  
Hamid Mala  
Xianping Mao  
Takahiro Matsuda  
Murat Moran  
Steven Murdoch  
Sean Murphy  
David Naccache  
Takashi Nishide  
Kazumasa Omote  
Goutam Paul  
Baodong Qin  
Elizabeth A. Quaglia  
Mohammad Reza Reyhanitabar  
Alfredo Rial  
Somitra Sanadhya  
Santanu Sarkar  
Patrick Schweitzer  
Michael Scott  
Sourav Sen Gupta  
Taizo Shirai  
Masaaki Shirase  
Riccardo Sisto  
Efsthios Stathakidis  
Graham Steel  
Koutarou Suzuki  
Katsuyuki Takashima  
Xiao Tan  
Qiang Tang  
Stefan Tillich  
Jheng-Hong Tu

Max Tuengerthal  
Joop Van De Pol  
Roel Verdult  
Andreas Vogt  
Daoshun Wang  
Jun Wang  
Liangliang Wang  
Yu Wang  
Gaven J. Watson  
Robert Watson  
Lingbo Wei  
Yongzhuang Wei  
Sheng Wen  
Gaoyao Xiao  
Zhi Xin  
Xi Xiong  
Yanjiang Yang  
Rehana Yasmin  
Tomoko Yonemura  
Ching-Hua Yu  
S. Yu  
Tsz Hon Yuen  
Greg Zaverucha  
Hailong Zhang  
Jun Zhang  
Shengzhi Zhang  
Wei Zhang  
Xusheng Zhang  
Zongyang Zhang  
Mingyi Zhao  
Bin Zhu



# Table of Contents

## Digital Signatures

A Pre-computable Signature Scheme with Efficient Verification for RFID .....	1
<i>Fuchun Guo, Yi Mu, Willy Susilo, and Vijay Varadharajan</i>	
Redactable Signatures for Independent Removal of Structure and Content .....	17
<i>Kai Samelin, Henrich C. Pöhls, Arne Bilzhaue, Joachim Posegga, and Hermann de Meer</i>	

## Public Key Cryptography

Improved Efficiency of Chosen Ciphertext Secure Encryption from Factoring .....	34
<i>Xianhui Lu, Bao Li, Qixiang Mei, and Yamin Liu</i>	
Deniable Encryptions Secure against Adaptive Chosen Ciphertext Attack.....	46
<i>Chong-zhi Gao, Dongqing Xie, and Baodian Wei</i>	
Computational Soundness of Indistinguishability Properties without Computable Parsing.....	63
<i>Hubert Comon-Lundh, Masami Hagiya, Yusuke Kawamoto, and Hideki Sakurada</i>	

## Cryptanalysis I: Differential Attacks

New Impossible Differential Attacks on Camellia .....	80
<i>Dongxia Bai and Leibo Li</i>	
Impossible Differential Attacks on Reduced-Round LBlock .....	97
<i>Ya Liu, Dawu Gu, Zhiqiang Liu, and Wei Li</i>	
New Truncated Differential Cryptanalysis on 3D Block Cipher .....	109
<i>Takuma Koyama, Lei Wang, Yu Sasaki, Kazuo Sakiyama, and Kazuo Ohta</i>	

## Applications I.i: Oblivious Transfer

T-out-of-n Distributed Oblivious Transfer Protocols in Non-adaptive and Adaptive Settings .....	126
<i>Christian L.F. Corniaux and Hossein Ghodosi</i>	

A Code-Based 1-out-of-N Oblivious Transfer Based on McEliece Assumptions .....	144
<i>Preetha Mathew K., Sachin Vasant, Sridhar Venkatesan, and C. Pandu Rangan</i>	

## Applications I.ii: Internet Security (Works-in-Progress)

Towards Fine-Grained Access Control on Browser Extensions .....	158
<i>Lei Wang, Ji Xiang, Jiwu Jing, and Lingchen Zhang</i>	
Enhanced STE3D-CAP: A Novel 3D CAPTCHA Family .....	170
<i>Yang-Wai Chow and Willy Susilo</i>	

## Key Management

High-Entropy Visual Identification for Touch Screen Devices .....	182
<i>Nathaniel Wesley Filardo and Giuseppe Ateniese</i>	
A Framework for Security Analysis of Key Derivation Functions .....	199
<i>Chuah Chai Wen, Edward Dawson, Juan Manuel González Nieto, and Leonie Simpson</i>	

## Applied Cryptography

On the Equivalence of Two Definitions of Visual Cryptography Scheme .....	217
<i>Teng Guo, Feng Liu, and ChuanKun Wu</i>	
Key Length Estimation of Pairing-Based Cryptosystems Using $\eta_T$ Pairing .....	228
<i>Naoyuki Shinohara, Takeshi Shimoyama, Takuya Hayashi, and Tsuyoshi Takagi</i>	
Lightweight Integrity for XOR Network Coding in Wireless Sensor Networks .....	245
<i>Kazuya Izawa, Atsuko Miyaji, and Kazumasa Omote</i>	

## Applications II.i: PINs

iPIN and mTAN for Secure eID Applications .....	259
<i>Johannes Braun, Moritz Horsch, and Alexander Wiesmaier</i>	

## Applications II.ii: Fundamentals (Works-in-Progress)

Secure Distributed Computation of the Square Root and Applications.....	277
<i>Manuel Liedel</i>	
Prevent Kernel Return-Oriented Programming Attacks Using Hardware Virtualization .....	289
<i>Tian Shuo, He Yeping, and Ding Baozeng</i>	

## Cryptanalysis II: Fault Attacks and Key Recovery

Structure-Based RSA Fault Attacks .....	301
<i>Benjamin Michéle, Juliane Krämer, and Jean-Pierre Seifert</i>	
Fault Analysis of the KATAN Family of Block Ciphers .....	319
<i>Shekh Faisal Abdul-Latip, Mohammad Reza Reyhanitabar, Willy Susilo, and Jennifer Seberry</i>	
Biclique Cryptanalysis of Reduced-Round Piccolo Block Cipher .....	337
<i>Yanfeng Wang, Wenling Wu, and Xiaoli Yu</i>	
On the CCA-1 Security of Somewhat Homomorphic Encryption over the Integers .....	353
<i>Zhenfei Zhang, Thomas Plantard, and Willy Susilo</i>	

## Cryptanalysis III: Key Recovery (Works-in-Progress)

Partial Key Exposure on RSA with Private Exponents Larger Than $N$ .....	369
<i>Marc Joye and Tancreède Lepoint</i>	
Linear Cryptanalysis of Reduced-Round ICEBERG .....	381
<i>Yue Sun and Meiqin Wang</i>	
Overcoming Significant Noise: Correlation-Template-Induction Attack.....	393
<i>An Wang, Man Chen, Zongyue Wang, and Yaoling Ding</i>	
<b>Author Index</b> .....	405