Lecture Notes in Computer Science 4856

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

Feng Bao San Ling Tatsuaki Okamoto
Huaxiong Wang Chaoping Xing (Eds.)

# Cryptology and Network Security

6th International Conference, CANS 2007
Singapore, December 8-10, 2007
Proceedings

Springer

Volume Editors

Feng Bao
Institute for Infocomm Research
Singapore
E-mail: baofeng@i2r.a-star.edu.sg

San Ling
Nanyang Technological University
Singapore
E-mail: lingsan@ntu.edu.sg

Tatsuaki Okamoto
NTT Laboratories
Japan
E-mail: okamoto.tatsuaki@lab.ntt.co.jp

Huaxiong Wang
Nanyang Technological University
Singapore
E-mail: hxwang@ntu.edu.sg

Chaoping Xing
Nanyang Technological University
Singapore
E-mail: matxcp@nus.edu.sg

Library of Congress Control Number: 2007939802

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-76968-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-76968-2 Springer Berlin Heidelberg New York



Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12196395 06/3180 5 4 3 2 1 0

# Preface

The sixth International Conference on Cryptology and Network Security (CANS 2007) was held at the Grand Plaza Park Hotel, Singapore, 8–10 December 2007. The conference was sponsored by *Nanyang Technological University* and the *Lee Foundation*, Singapore.

The goal of CANS is to promote research on all aspects of cryptology and network security, as well as to build a bridge between research on cryptography and network security. The first International Conference on Cryptology and Network Security was held in Taipei, Taiwan, in 2001. The second one was held in San Francisco, California, USA, on September 26–28, 2002, the third in Miami, Florida, USA, on September 24–26, 2003, the fourth in Xiamen, Fujian, China, on December 14–16, 2005 and the fifth in Suzhou, Jiangsu, China, on December 8–10, 2006.

The program committee accepted 17 papers from 68 submissions. The reviewing process took nine weeks, each paper was carefully evaluated by at least three members of the program committee. We appreciate the hard work of the members of the program committee and the external referees who gave many hours of their valuable time.

In addition to the contributed papers, there were six invited talks:

- Artur Ekert: *Quantum Cryptography*
- Christian Kurtsiefer: *Aspects of Practical Quantum Key Distribution Schemes*
- Keith Martin: *A Bird's-Eye View of Recent Research in Secret Sharing*
- Mitsuru Matsui: *The State-of-the-Art Software Optimization of Block Ciphers and Hash Functions*
- Josef Pieprzyk: *Analysis of Modern Stream Ciphers*
- David Pointcheval: *Adaptive Security for Password-Based Authenticated Key Exchange in the Universal-Composability Framework.*

We would like to thank all the people involved in organising this conference. In particular, we would like to thank the organising committee for their time and efforts, and Krystian Matusiewicz for his help with LaTeX.

December 2007

Feng Bao
San Ling
Tatsuaki Okamoto
Huaxiong Wang
Chaoping Xing

# 6th International Conference on Cryptology and Network Security (CANS 2007)

Sponsored by

Nanyang Technological University, Singapore
Lee Foundation, Singapore

## CANS Steering Committee

| | |
|---|---|
| Yvo Desmedt | University College London, UK |
| Matt Franklin | UC, David, USA |
| Yi Mu | University of Wollongong, Australia |
| David Pointcheval | CNRS and ENS, France |
| Huaxiong Wang | Nanyang Technological University, Singapore |

## General Chairs

| | |
|---|---|
| San Ling | Nanyang Technological University, Singapore |
| Chaoping Xing | National University of Singapore, Singapore |

## Program Chairs

| | |
|---|---|
| Feng Bao | Institute for Infocomm Research, Singapore |
| Tatsuaki Okamoto | NTT Labs, Japan |

## Program Committee

| | |
|---|---|
| Michel Abdalla | École Normale Supérieure, France |
| Colin Boyd | QUT, Australia |
| Mike Burmester | Florida State University, USA |
| Hao Chen | Fudan University, China |
| Liqun Chen | HP Bristol Labs, UK |
| Robert Deng | SMU, Singapore |
| Alex Dent | Royal Holloway, UK |
| Eiichiro Fujisaki | NTT Labs, Japan |
| Jun Furukawa | NEC, Japan |
| David Galindo | École Normale Supérieure, France |
| Aline Gouget | Gemalto, France |
| Amir Herzberg | Bar Ilan University, Israel |

| | |
|---|---|
| Atsuo Inomata | JST, Japan |
| Akinori Kawachi | Titech, Japan |
| Angelos Keromytis | Columbia University |
| Aggelos Kiayias | University of Connecticut, USA |
| Hiroaki Kikuchi | Tokai University, Japan |
| Eike Kiltz | CWI, Netherlands |
| Kwangjo Kim | Info. and Comm. University, Korea |
| Arjen Lenstra | EPFL, Switzerland |
| Peng Chor Leong | NTU, Singapore |
| Javier Lopez | University of Malaga, Spain |
| Mitsuru Matsui | Mitsubishi Electric, Japan |
| Yi Mu | University of Wollongong, Australia |
| Joern Mueller-Quade | University of Karlsruhe, Germany |
| Antonio Nicolosi | NYU & Stanford University, USA |
| Kenny Paterson | Royal Holloway, UK |
| Olivier Pereira | UCL, Belgium |
| Giuseppe Persiano | Università di Salerno, Italy |
| Josef Pieprzyk | Macquarie University, Australia |
| C. Pandu Rangan | IIT, India |
| Frederic Rousseau | EADS, France |
| Rei Safavi-Naini | University of Calgary, Canada |
| Berry Schoenmakers | TU Eindhoven, Netherlands |
| Jorge Villar | Universitat Politècnica de Catalunya, Spain |
| Xiaoyun Wang | Shandong University, China |
| Duncan Wong | City University of Hong Kong, China |
| Sung-Ming Yen | National Central University, Taiwan |
| Yiqun Lisa Yin | Security Consultant, USA |
| Yunlei Zhao | Fudan University, China |
| Jianying Zhou | $I^2R$, Singapore |

## Organising Committee

| | |
|---|---|
| Huaxiong Wang | Nanyang Technological University, Singapore |
| Eiji Okamoto | Tsukuba, Japan |
| Guat Tin Goh | Nanyang Technological University, Singapore |
| Hwee Jin Soh | Nanyang Technological University, Singapore |
| Sen How Chia | Nanyang Technological University, Singapore |

## External Referees

| | | |
|---|---|---|
| Frederik Armknecht | Scott Contini | Eiichiro Fujisaki |
| Sébastien Canard | Cunsheng Ding | Steven Galbraith |
| Kai Yuen Cheong | Gerardo Fernandez | Clemente Galdi |
| Benoit Chevallier-Mames | Pierre-Alain Fouque | Paul Hoffman |

Qiong Huang
Tetsu Iwata
Shaoquan Jiang
Marcelo Kaihara
Tomi Klein
David Lacour
Byoungcheon Lee
Homin K. Lee
Wei-Chih Lien
Benoit Libert
Krystian Matusiewicz
Cedric Ng
Juan Gonzalez Nieto
Christopher Portmann
Geraint Price
M-R Reyhanitabar
Stefan Röhrich
Ryo Sakaguchi
Siamak F. Shahandashti
Tom Shrimpton
Martijn Stam
Kohtaro Tadaki
Qian Tang
Jheng-Hong Tu
Marion Videau
Nguyen Vo
Martin Vuagnoux
Bo-Ching Wu
Chi-Dian Wu
Qianhong Wu
Chih-Hung Wang
Guomin Yang
Kan Yasuda
Hong-Sheng Zhou

# Table of Contents

## Signatures



## Network Security



## Secure Keyword Search and Private Information Retrieval

## Public Key Encryption



## Intrusion Detection



## Email Security



## Denial of Service Attacks



## Authentication