

*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*

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

*University of Dortmund, Germany*

Madhu Sudan

*Massachusetts Institute of Technology, MA, USA*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Moshe Y. Vardi

*Rice University, Houston, TX, USA*

Gerhard Weikum

*Max-Planck Institute of Computer Science, Saarbruecken, Germany*

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

## 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

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 is a part of Springer Science+Business Media  
springer.com

© Springer-Verlag Berlin Heidelberg 2007  
Printed in Germany

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 L<sup>A</sup>T<sub>E</sub>X.

December 2007

Feng Bao  
San Ling  
Tatsuaki Okamoto  
Huaxiong Wang  
Chaoping Xing

# **6<sup>th</sup> 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
Eiichi 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 <sup>2</sup> R, Singapore

## Organising Committee

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

# Table of Contents

## Signatures

Mutative Identity-Based Signatures or Dynamic Credentials Without Random Oracles .....	1
<i>Fuchun Guo, Yi Mu, and Zhide Chen</i>	
A Generic Construction for Universally-Convertible Undeniable Signatures .....	15
<i>Xinyi Huang, Yi Mu, Willy Susilo, and Wei Wu</i>	
Fast Digital Signature Algorithm Based on Subgraph Isomorphism .....	34
<i>Loránd Szöllősi, Tamás Marosits, Gábor Fehér, and András Recski</i>	
Efficient ID-Based Digital Signatures with Message Recovery .....	47
<i>Raylin Tso, Chunxiang Gu, Takeshi Okamoto, and Eiji Okamoto</i>	

## Network Security

Achieving Mobility and Anonymity in IP-Based Networks .....	60
<i>Rungrat Wiangsripanawan, Willy Susilo, and Rei Safavi-Naini</i>	
Perfectly Secure Message Transmission in Directed Networks Tolerating Threshold and Non Threshold Adversary .....	80
<i>Arpita Patra, Bhavani Shankar, Ashish Choudhary, K. Srinathan, and C. Pandu Rangan</i>	
Forward-Secure Key Evolution in Wireless Sensor Networks .....	102
<i>Marek Klonowski, Mirosław Kutylowski, Michał Ren, and Katarzyna Rybarczyk</i>	
A Secure Location Service for Ad Hoc Position-Based Routing Using Self-signed Locations .....	121
<i>Jihwan Lim, Sangjin Kim, and Heekuck Oh</i>	
An Intelligent Network-Warning Model with Strong Survivability .....	133
<i>Bing Yang, Huaping Hu, Xiangwen Duan, and Shiyao Jin</i>	
Running on Karma – P2P Reputation and Currency Systems .....	146
<i>Sherman S.M. Chow</i>	

## Secure Keyword Search and Private Information Retrieval

Generic Combination of Public Key Encryption with Keyword Search and Public Key Encryption .....	159
<i>Rui Zhang and Hideki Imai</i>	



Extended Private Information Retrieval and Its Application in Biometrics Authentications .....	175
<i>Julien Bringer, Hervé Chabanne, David Pointcheval, and Qiang Tang</i>	

## Public Key Encryption

Strongly Secure Certificateless Public Key Encryption Without Pairing .....	194
<i>Yinxia Sun, Futai Zhang, and Joonsang Baek</i>	

## Intrusion Detection

Modeling Protocol Based Packet Header Anomaly Detector for Network and Host Intrusion Detection Systems .....	209
<i>Solahuddin B. Shamsuddin and Michael E. Woodward</i>	

## Email Security

How to Secure Your Email Address Book and Beyond .....	228
<i>Erhan J. Kartaltepe, T. Paul Parker, and Shouhuai Xu</i>	

## Denial of Service Attacks

Toward Non-parallelizable Client Puzzles .....	247
<i>Suratose Tritilanunt, Colin Boyd, Ernest Foo, and Juan Manuel González Nieto</i>	

## Authentication

Anonymity 2.0 – X.509 Extensions Supporting Privacy-Friendly Authentication .....	265
<i>Vicente Benjumea, Seung Geol Choi, Javier Lopez, and Moti Yung</i>	

Author Index .....	283
--------------------	-----