Lecture Notes in Computer Science 4301

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

David Pointcheval Yi Mu
Kefei Chen (Eds.)

Cryptology and Network Security

5th International Conference, CANS 2006
Suzhou, China, December 8-10, 2006
Proceedings

Springer

Volume Editors

David Pointcheval
CNRS, École Normale Supérieure
Paris, France
E-mail: David.Pointcheval@ens.fr

Yi Mu
Center for Information Security Research
SITACS, University of Wollongong
Wollongong NSW 2522, Australia
E-mail: ymu@uow.edu.au

Kefei Chen
Dept. of Computer Science and Engineering
Shanghai Jiaotong University
Shanghai 200240, P.R., China
E-mail: kfchen@sjtu.edu.cn

Library of Congress Control Number: 2006937156

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 3-540-49462-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-49462-1 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11935070 06/3142 5 4 3 2 1 0

Preface

The fifth International Conference on Cryptology and Network Security (CANS 2006) was held in Suzhou, Jiangsu, China, December 8–10, 2006. The conference was organized in cooperation with the International Association for Cryptologic Research (IACR) and the National Nature Science Foundation of China (NSFC).

The 1st International Workshop on Cryptology and Network Security was held in Taipei, Taiwan, 2001. The second one was in San Francisco, California, USA, September 26-28, 2002, the third in Miami, Florida, USA, September 24-26, 2003, and the fourth in Xiamen, Fujian Province, China, December 14-16, 2005. CANS 2005 was the first CANS with proceedings published in the *Lecture Notes in Computer Science* series by Springer and granted the success of last year and this year, CANS 2006 was also published in the same series. The Program Committee received 148 submissions, and accepted 26 papers, all included in the proceedings.

The reviewing process, which took eight weeks, was run using the iChair software, written by Thomas Baignères and Matthieu Finiasz (EPFL, Switzerland). Each paper was carefully evaluated by at least three members from the Program Committee. We appreciate the hard work of the members of the Program Committee and external referees who gave many hours of their valuable time.

Note that these proceedings contain the revised versions of the selected papers. Since the revisions were not checked again before publication, the authors (and not the committee) bear full responsibility of the contents of their papers.

In addition to the contributed papers, there were two invited talks: Moni Naor and Xiaoyun Wang.

We would like to thank all the people involved in organizing this conference. In particular we would like to thank the General Chair, Kefei Chen, the Co-chairs of the Organizing Committee Dong Zheng and Weidong Qiu, and people from the Shanghai Jaotong University for their time and efforts.

Finally, we wish to thank all the authors who submitted papers, and the authors of accepted papers for sending their final versions on time.

December 2006

David Pointcheval
Yi Mu
Kefei Chen

Fifth International Conference on Cryptology and Network Security (CANS 2005)

In Cooperation with
The International Association for Cryptologic Research (IACR)

Sponsored by
Shanghai Jiao Tong University (SJTU), China
National Nature Science Foundation of China (NSFC)

General Chair

Kefei Chen ..... Shanghai Jaotong University, China

Program Chairs

Yi Mu ..... University of Wollongong, Australia
David Pointcheval ..... CNRS and ENS, France

Program Committee

Farooq Anjum ..... Telcordia, USA
Feng Bao ..... Institute for Infocomm Research, Singapore
Christophe Bidan ..... Supélec, France
John Black ..... University of Colorado, USA
Carlo Blundo ..... Università di Salerno, Italy
Colin Boyd ..... QUT, Australia
Xavier Boyen ..... Voltage, USA
Laurent Bussard ..... EMIC, Germany
Liqun Chen ..... HP Laboratories, UK
Anand Desai ..... NTT MCL, USA
Cunsheng Ding ..... Hong Kong Univ. Sci. Tech., China
Steven Galbraith ..... Royal Holloway Univ. of London, UK
Marc Girault ..... France Telecom, France
Nick Howgrave-Graham ..... NTRU Cryptosystems, USA
Marc Joye ..... Thomson R&D, France
Kwangjo Kim ..... ICU, South Korea
Kaoru Kurosawa ..... Ibaraki University, Japan
Xuejia Lai ..... Shanghai Jiao Tong University, China
Dong Hoon Lee ..... Korea University, South Korea
Arjen Lenstra ..... EPFL, Switzerland

Javier Lopez ..... University of Malaga, Spain
Atsuko Miyaji ..... JAIST, Japan
David Naccache ..... ENS and University of Paris II, France
Kaisa Nyberg ..... TU of Helsinki and Nokia, Finland
Giuseppe Persiano ..... Università di Salerno, Italy
Josef Pieprzyk ..... Macquarie University, Australia
C.-Pandu Rangan ..... Indian Institute of Technology, India
Kazue Sako ..... NEC, Japan
Berry Schoenmakers ..... TU Eindhoven, Netherlands
Willy Susilo ..... University of Wollongong, Australia
Vijay Varadharajan ..... Macquarie University, Australia
Xiaofeng Wang ..... Indiana University, USA
Duncan Wong ..... City University of Hong Kong, China
Chaoping Xing ..... National Univ. of Singapore, Singapore
Shouhuai Xu ..... University of Texas, USA
Sung-Ming Yen ..... National Central Univ., Taiwan

Organizing Committee

Dong Zheng (Chair) ..... Shanghai Jiaotong University, China
Weidong Qiu (Chair) ..... Shanghai Jiaotong University, China
Zheng Huang ..... Shanghai Jiaotong University, China
Shengli Liu ..... Shanghai Jiaotong University, China
Jie Guo ..... Shanghai Jiaotong University, China

External Referees

Patrick Amon
Toshinori Araki
Roberto Avanzi
Pedro Bados Aguilar
Chris Charnes
Jing Chen
Xiaofeng Chen
Benoît Chevallier-Mames
Bessie C. Hu
Carlos Cid
Yang Cui
Paolo D'Arco
Alex Dent
Hiroshi Doi
Gerardo Fernandez
Jun Furukawa
Clemente Galdi
Changzhe Gao
Juan Gonzalez
Vanessa Gratzer
Gaurav Gupta
Goichiro Hanaoka
Matt Henricksen
Guillaume Hiet
Paul Hoffman
Chao-Chih Hsu
Xinyi Huang
Toshiyuki Isshiki
Erhan Kartaltepe
Hiroaki Kikuchi
Mehmet Kiraz
Yuichi Komano
Jérôme Lebègue
Tieyan Li
Zhuowei Li
Benoît Libert
Wei-Chih Lien
Hsi-Chung Lin
Liang Lu
Ludovic Mé
Miao Ma
Frédéric Majorczyk
Toshihiko Matsuo
Krystian Matusiewicz
Kengo Mori
Benjamin Morin
Sean Murphy
Satoshi Obana

Tatsuaki Okamoto
Dag Arne Osvik
Dan Page
Pascal Paillier
Kenny Paterson
Rodrigo Roman
Nicholas Sheppard
Martijn Stam
Ye Tang
Christophe Tartary
Isamu Teranishi
Xiaojian Tian
Rafael Timóteo de Sousa Júnior
Eric Totel
Udaya Kiran Tupakula
Lionel Victor
Jos Villegas
Ivan Visconti
Kumar Viswanath
Huaxiong Wang
William Whyte
Robert W. Zhu
Shidi Xu
Guomin Yang
Dennis Y. W. Liu
Bo Zhu

Table of Contents

Encryption

Key Exchange

Authentication and Signatures

Proxy Signatures

Cryptanalysis

Implementation

Steganalysis and Watermarking

Boolean Functions and Stream Ciphers

Intrusion Detection

Disponibility and Reliability