

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

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

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 2006
Printed in Germany

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

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

Table of Contents

Encryption

Concrete Chosen-Ciphertext Secure Encryption from Subgroup Membership Problems	1
<i>Jaimee Brown, Juan Manuel González Nieto, Colin Boyd</i>	
Efficient Identity-Based Encryption with Tight Security Reduction	19
<i>Nuttapong Attrapadung, Jun Furukawa, Takeshi Gomi, Goichiro Hanaoka, Hideki Imai, Rui Zhang</i>	

Key Exchange

A Diffie-Hellman Key Exchange Protocol Without Random Oracles	37
<i>Ik Rae Jeong, Jeong Ok Kwon, Dong Hoon Lee</i>	
Authenticated Group Key Agreement for Multicast	55
<i>Liming Wang, Chuan-Kun Wu</i>	
Authenticated and Communication Efficient Group Key Agreement for Clustered Ad Hoc Networks	73
<i>Hongsong Shi, Mingxing He, Zhiguang Qin</i>	

Authentication and Signatures

Efficient Mutual Data Authentication Using Manually Authenticated Strings	90
<i>Sven Laur, Kaisa Nyberg</i>	
Achieving Multicast Stream Authentication Using MDS Codes	108
<i>Christophe Tartary, Huaxiong Wang</i>	
Shorter Verifier-Local Revocation Group Signatures from Bilinear Maps	126
<i>Sujing Zhou, Dongdai Lin</i>	

Proxy Signatures

Security Model of Proxy-Multi Signature Schemes	144
<i>Feng Cao, Zhenfu Cao</i>	

Efficient ID-Based One-Time Proxy Signature and Its Application in E-Cheque	153
<i>Rongxing Lu, Zhenfu Cao, Xiaolei Dong</i>	

Cryptanalysis

Side Channel Attacks and Countermeasures on Pairing Based Cryptosystems over Binary Fields	168
<i>Tae Hyun Kim, Tsuyoshi Takagi, Dong-Guk Han, Ho Won Kim, Jongin Lim</i>	
Improved Collision Attack on Reduced Round Camellia	182
<i>Jie Guan, Zhongya Zhang</i>	
Stealing Secrets with SSL/TLS and SSH – Kleptographic Attacks	191
<i>Zbigniew Golebiewski, Mirosław Kutylowski, Filip Zagórski</i>	

Implementation

Bitslice Implementation of AES	203
<i>Chester Rebeiro, David Selvakumar, A.S.L. Devi</i>	
A Fast Algorithm for Determining the Linear Complexity of Periodic Sequences over $GF(3)$	213
<i>Jianqin Zhou, Qiang Zheng</i>	

Steganalysis and Watermarking

Steganalysis Based on Differential Statistics	224
<i>Zugen Liu, Lingdi Ping, Jian Chen, Jimin Wang, Xuezeng Pan</i>	
Watermarking Essential Data Structures for Copyright Protection	241
<i>Qutaiba Albluwi, Ibrahim Kamel</i>	

Boolean Functions and Stream Ciphers

A Note of Perfect Nonlinear Functions	259
<i>Xiyong Zhang, Hua Guo, Jinjiang Yuan</i>	
Chaotic Keystream Generator Using Coupled NDFs with Parameter Perturbing	270
<i>Xiaomin Wang, Jiashu Zhang, Wenfang Zhang</i>	

Intrusion Detection

Cooperative Intrusion Detection for Web Applications	286
<i>Nathalie Dagorn</i>	
Finding TCP Packet Round-Trip Time for Intrusion Detection: Algorithm and Analysis	303
<i>Jianhua Yang, Byong Lee, Yongzhong Zhang</i>	
Smart Architecture for High-Speed Intrusion Detection and Prevention Systems	318
<i>Chih-Chiang Wu, Sung-Hua Wen, Nen-Fu Huang</i>	
A Multi-agent Cooperative Model and System for Integrated Security Monitoring	329
<i>Xianxian Li, Lijun Liu</i>	

Disponibility and Reliability

Detecting DDoS Attacks Based on Multi-stream Fused HMM in Source-End Network	342
<i>Jian Kang, Yuan Zhang, Jiu-bin Ju</i>	
An Immune-Based Model for Service Survivability	354
<i>Jinquan Zeng, Xiaojie Liu, Tao Li, Feixian Sun, Lingxi Peng, Caiming Liu</i>	
X ² BT Trusted Reputation System:A Robust Mechanism for P2P Networks	364
<i>Lan Yu, Willy Susilo, Rei Safavi-Naini</i>	
Author Index	381