Lecture Notes in Computer Science 5888

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 of Computer Science, Saarbruecken, Germany

Juan A. Garay Atsuko Miyaji
Akira Otsuka (Eds.)

Cryptology and Network Security

8th International Conference, CANS 2009
Kanazawa, Japan, December 12-14, 2009
Proceedings

Springer

Volume Editors

Juan A. Garay
AT&T Labs Research
Florham Park, NJ, USA
E-mail: garay@research.att.com

Atsuko Miyaji
Japan Advanced Institute of Science and Technology (JAIST)
Nomi, Ishikawa, Japan
E-mail: miyaji@jaist.ac.jp

Akira Otsuka
National Institute of Advanced Industrial Science and Technoloy (AIST)
Tokyo, Japan
E-mail: a-otsuka@aist.go.jp

Library of Congress Control Number: 2009939618

CR Subject Classification (1998): E.3, G.2, D.4.6, K.6.5, C.2, E.4, K.4.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-10432-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-10432-9 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.com

© Springer-Verlag Berlin Heidelberg 2009
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12799756 06/3180 5 4 3 2 1 0

Preface

The 8th International Conference on Cryptology and Network Security (CANS 2009) was held at the Ishikawa Prefectural Museum of Art in Kanazawa, Japan, during December 12–14, 2009. The conference was jointly co-organized by the National Institute of Advanced Industrial Science and Technology (AIST), Japan, and the Japan Advanced Institute of Science and Technology (JAIST). In addition, the event was supported by the Special Interest Group on Computer Security (CSEC), IPSJ, Japan, the Japan Technical Group on Information Security (ISEC), IEICE, the Japan Technical Committee on Information and Communication System Security(ICSS), IEICE, and the Society of Information Theory and its Applications (SITA), Japan, and co-sponsored by the National Institute of Information and Communications Technology, Japan, ComWorth Co., LTD, Japan, Hitachi, Ltd., Hokuriku Telecommunication Network Co.,Inc., and Internet Initiative Japan Inc.

The conference received 109 submissions from 24 countries, out of which 32 were accepted for publication in these proceedings. At least three Program Committee (PC) members reviewed each submitted paper, while submissions co-authored by a PC member were submitted to the more stringent evaluation of five PC members. In addition to the PC members, many external reviewers joined the review process in their particular areas of expertise. We were fortunate to have this energetic team of experts, and are deeply grateful to all of them for their hard work, which included a very active discussion phase—almost as long as the initial individual reviewing period. The paper submission, review and discussion processes were effectively and efficiently made possible by the Web-based system iChair.

The main goal of CANS as a conference is to promote research on all aspects of network security, as well as to build a bridge between research on cryptology and on network security. The broad range of areas covered by the high-quality accepted papers to the current edition, which include novel cryptographic and number-theoretic constructs enabling new functionalities, the various security aspects of protocols and wireless and sensor networks, new cipher designs, advanced cryptanalytic techniques without which soundness would be unattainable, and the treatment of privacy in multifarious settings, from privacy-preserving computation to privacy in the ever-popular social networks, attests—exceedingly—to the fulfillment of that goal. In addition, the conference featured three invited speakers: Craig Gentry from IBM Research, Adrian Perrig from Carnegie Mellon University, and Adam Smith from The Pennsylvania State University, whose lectures on cutting-edge research areas—"Computing on Encrypted Data," "Building Secure Networked Systems with Code Attestation," and "A Cryptographer's-Eye View of Privacy in Statistical Databases," respectively—contributed in no small part to the richness of the program.

Finally, we thank all the authors who submitted papers to this conference; the Organizing Committee members, colleagues and student helpers for their valuable time and effort; and all the conference attendees who made this event a truly intellectually stimulating one through their active participation.

December 2009

Juan A. Garay
Atsuko Miyaji
Akira Otsuka

CANS 2009
8th International Conference on Cryptology and Network Security

Jointly organized by

National Institute of Advanced Industrial Science and Technology (AIST)
and
Japan Advanced Institute of Science and Technology (JAIST).

General Chair

Akira Otsuka (AIST, Japan)

Program Co-chairs

Juan A. Garay (AT&T Labs - Research, USA)
Atsuko Miyaji (JAIST, Japan)

Organizing Committee

Local Arrangements Co-chairs	Kazumasa Omote (JAIST, Japan)
	Shoichi Hirose (University of Fukui, Japan)
	Yuji Suga (IIJ, Japan)
	Natsume Matsuzaki (Panasonic, Japan)
Finance Co-chairs	Katsuyuki Takashima (Mitsubishi Electric, Japan)
	Shoko Yonezawa (AIST, Japan)
Publicity Co-chairs	Tomoyuki Asano (Sony, Japan)
	Daisuke Inoue (NICT, Japan)
	Kensuke Shibata (NTT Labs, Japan)
Liaison Co-chairs	Keisuke Takemori (KDDI R&D Labs., Japan)
	Shinichiro Matsuo (NICT, Japan)
System Co-chairs	Atsuo Inomata (NAIST, Japan)
	Yutaka Oiwa (AIST, Japan)
	Takao Ogura (Fujitsu Laboratories, Japan)
	Toshihiro Tabata (Okayama University, Japan)
Publication Co-chairs	Isao Echizen (NII, Japan)
	Takeshi Okamoto (Tsukuba University of Technology, Japan)
Registration Co-chairs	Tatsuyuki Matsushita (Toshiba, Japan)
	Kunihiko Miyazaki (Hitachi, Japan)

Program Committee

Jean-Luc Beuchat	University of Tsukuba, Japan
Alexandra Boldyreva	Georgia Institute of Technology, USA
Colin Boyd	Queensland University of Technology, Australia
Emmanuel Bresson	DCSSI Crypto Lab, France
Mike Burmester	FSU, USA
Koji Chida	NTT Labs, Japan
Ee-Chien Chang	National University of Singapore, Singapore
Rosario Gennaro	IBM T.J. Watson Research Center, USA
Trevor Jim	AT&T Labs - Research, USA
Charanjit Jutla	IBM T.J. Watson Research Center, USA
Seny Kamara	Microsoft Research, USA
Aggelos Kiayias	UConn, USA
Vladimir Kolesnikov	Bell Labs, USA
Tanja Lange	Technical University Eindhoven, The Netherlands
Dong Hoon Lee	Korea University, Korea
Pil Joong Lee	Pohang University of Science and Technology, Korea
Benoit Libert	UCL, Belgium
Helger Lipmaa	Cybernetica AS, Estonia
Subhamoy Maitra	Indian Statistical Institute, India
Mark Manulis	TU Darmstadt, Germany
David Nowak	AIST, Japan
Wakaha Ogata	Tokyo Institute of Technology, Japan
C. Pandu Rangan	IIT Madras, India
Kenny Paterson	Royal Holloway, University of London, UK
Rene Peralta	NIST, USA
Josef Pieprzyk	Macquarie University, Australia
German Saez	UPC, Spain
Taizo Shirai	Sony, Japan
Adam Smith	Penn State University, USA
Jessica Staddon	PARC, USA
Douglas Stinson	University of Waterloo, Canada
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	Future University - Hakodate, Japan
Gene Tsudik	UC Irvine, USA
Ivan Visconti	University of Salerno, Italy
Xiaoyun Wang	Shandong University, China
Duncan S. Wong	City University of Hong Kong, China
Sung-Ming Yen	National Central University, Taiwan
Hong-Sheng Zhou	UConn, USA
Jianying Zhou	I2R, Singapore

External Reviewers

Man Ho Au, Toru Akishita, Franz Baader, Lucas Ballard, Paulo Barreto, Rebecca Braynard, Luigi Catuogno, Nishanth Chandran, Chien-Ning Chen, Joo Yeon Cho, Kwan Tae Cho, Sherman Chow, Cheng-Kang Chu, Ji Young Chun, Baudoin Collard, Emiliano De Cristofaro, Giovanni Di Crescenzo, Vanesa Daza, Karim El Defrawy, Yvo Desmedt, Jérémie Detrey, Xuhua Ding, Orr Dunkelman, Lei Fan, Pierre-Alain Fouque, Thomas Fuhr, David Galindo, Hossein Ghodosi, Jon Giffin, Juan Gonzalez, Choudary Gorantla, Matthew Green, Gerhard Hancke, Shoichi Hirose, Jin Hong, Xinyi Huang, Dai Ikarashi, Yuto Kawahara, Jun Kurihara, Bum Han Kim, Jihye Kim, Ki Tak Kim, Sun Young Kim, Woo Kwon Koo, Simon Kramer, Jun Kurihara, Jun Ho Lee, Wei-Chih Lien, Hsi-Chung Lin, Joseph K. Liu, Yanbin Lu, Vadim Lyubashevsky, Di Ma, Francesco Matarazzo, Daniele Micciancio, Marine Minier, Chris J. Mitchell, Shiho Moriai, Paz Morillo, Benjamin Morin, Mridul Nandi, Ching Yu Ng, Yasuyuki Nogami, Mehrdad Nojoumian, Adam O'Neill, Jung Ha Paik, Prabal Paul, Souradyuti Paul, Sean Peisert, Olivier Pereira, Ludovic Perret, Fabio Petagna, Le Trieu Phong, Benny Pinkas, Bertram Poettering, Axel Poschmann, Carla Rafols, Dominik Raub, Mariana Raykova, Mathieu Renauld, Hyun Sook Rhee, Francisco Rodríguez- Henríquez, Arnab Roy, Markus Ruckert, Alexandre Ruiz, Koichi Sakumoto, Palash Sarkar, Dominique Schroeder, Jae Woo Seo, Elaine Shi, Kyoji Shibutani, Masaaki Shirase, Jason Smith, Francois-Xavier Standaert, Hidema Tanaka, Toshiaki Tanaka, Ersin Uzun, Frederik Vercauteren, Marion Videau, Nguyen Vo, Christian Wachsmann, Bogdan Warinschi, Dai Watanabe, Hao-Chi Wong, Xiaokang Xiong, Yeon-Hyeong Yang, Yanjiang Yang, Tsz Hon Yuen, Greg Zaverucha, Fan Zhang.

Table of Contents

Cryptographic Protocol and Schemes I

Improved Garbled Circuit Building Blocks and Applications to Auctions and Computing Minima 1
Vladimir Kolesnikov, Ahmad-Reza Sadeghi, and Thomas Schneider

Multi Party Distributed Private Matching, Set Disjointness and Cardinality of Set Intersection with Information Theoretic Security 21
G. Sathya Narayanan, T. Aishwarya, Anugrah Agrawal, Arpita Patra, Ashish Choudhary, and C. Pandu Rangan

On Cryptographic Schemes Based on Discrete Logarithms and Factoring 41
Marc Joye

Invited Talk 1

Asymptotically Optimal and Private Statistical Estimation 53
Adam Smith

Cryptanalysis I

Linear (Hull) and Algebraic Cryptanalysis of the Block Cipher PRESENT 58
Jorge Nakahara Jr., Pouyan Sepehrdad, Bingsheng Zhang, and Meiqin Wang

Saturation Attack on the Block Cipher HIGHT 76
Peng Zhang, Bing Sun, and Chao Li

Extensions of the Cube Attack Based on Low Degree Annihilators 87
Aileen Zhang, Chu-Wee Lim, Khoongming Khoo, Lei Wei, and Josef Pieprzyk

An Analysis of the Compact XSL Attack on BES and Embedded SMS4 103
Jiali Choy, Huihui Yap, and Khoongming Khoo

Wireless and Sensor Network Security I

RFID Distance Bounding Protocol with Mixed Challenges to Prevent Relay Attacks 119
Chong Hee Kim and Gildas Avoine

Anonymizer-Enabled Security and Privacy for RFID 134
Ahmad-Reza Sadeghi, Ivan Visconti, and Christian Wachsmann

Blink 'Em All: Scalable, User-Friendly and Secure Initialization of Wireless Sensor Nodes 154
Nitesh Saxena and Md. Borhan Uddin

Network Security

DepenDNS: Dependable Mechanism against DNS Cache Poisoning 174
Hung-Min Sun, Wen-Hsuan Chang, Shih-Ying Chang, and Yue-Hsun Lin

Privacy and Anonymity

Privacy-Preserving Relationship Path Discovery in Social Networks 189
Ghita Mezzour, Adrian Perrig, Virgil Gligor, and Panos Papadimitratos

Verifying Anonymous Credential Systems in Applied Pi Calculus 209
Xiangxi Li, Yu Zhang, and Yuxin Deng

Transferable Constant-Size Fair E-Cash 226
Georg Fuchsbauer, David Pointcheval, and Damien Vergnaud

Functional and Searchable Encryption

A Secure Channel Free Public Key Encryption with Keyword Search Scheme without Random Oracle 248
Liming Fang, Willy Susilo, Chunpeng Ge, and Jiandong Wang

Private-Key Hidden Vector Encryption with Key Confidentiality 259
Carlo Blundo, Vincenzo Iovino, and Giuseppe Persiano

Invited Talk 2

Building Secure Networked Systems with Code Attestation (Abstract) 278
Adrian Perrig

Authentication

HPAKE : Password Authentication Secure against Cross-Site User Impersonation 279
Xavier Boyen

An Efficient and Provably Secure Cross-Realm Client-to-Client Password-Authenticated Key Agreement Protocol with Smart Cards ... 299
Wenting Jin and Jing Xu

Ensuring Authentication of Digital Information Using Cryptographic Accumulators ... 315
Christophe Tartary

Block Cipher Design

MIBS: A New Lightweight Block Cipher ... 334
Maryam Izadi, Babak Sadeghiyan, Seyed Saeed Sadeghian, and Hossein Arabnezhad Khanooki

Cryptanalysis II

Distinguishing and Second-Preimage Attacks on CBC-Like MACs ... 349
Keting Jia, Xiaoyun Wang, Zheng Yuan, and Guangwu Xu

Improving the Rainbow Attack by Reusing Colours ... 362
Martin Ågren, Thomas Johansson, and Martin Hell

Side Channel Cube Attack on PRESENT ... 379
Lin Yang, Meiqin Wang, and Siyuan Qiao

Algebraic Attack on the MQQ Public Key Cryptosystem ... 392
Mohamed Saied Emam Mohamed, Jintai Ding, Johannes Buchmann, and Fabian Werner

Algebraic and Number-Theoretic Schemes

Construction of Rotation Symmetric Boolean Functions with Maximum Algebraic Immunity ... 402
Shaojing Fu, Chao Li, Kanta Matsuura, and Longjiang Qu

Multi-core Implementation of the Tate Pairing over Supersingular Elliptic Curves ... 413
Jean-Luc Beuchat, Emmanuel López-Trejo, Luis Martínez-Ramos, Shigeo Mitsunari, and Francisco Rodríguez-Henríquez

On the Complexity of Computing Discrete Logarithms over Algebraic Tori ... 433
Shuji Isobe, Eisuke Koizumi, Yuji Nishigaki, and Hiroki Shizuya

Wireless and Sensor Network Security II

On the Usability of Secure Association of Wireless Devices Based on Distance Bounding ... 443
Mario Cagalj, Nitesh Saxena, and Ersin Uzun

Short Hash-Based Signatures for Wireless Sensor Networks 463
Erik Dahmen and Christoph Krauß

Invited Talk 3

Computing on Encrypted Data (Abstract) 477
Craig Gentry

Cryptographic Protocol and Schemes II

Fully Robust Tree-Diffie-Hellman Group Key Exchange 478
Timo Brecher, Emmanuel Bresson, and Mark Manulis

Group Signatures with Verifier-Local Revocation and Backward Unlinkability in the Standard Model 498
Benoît Libert and Damien Vergnaud

Relinkable Ring Signature 518
Koutarou Suzuki, Fumitaka Hoshino, and Tetsutaro Kobayashi

Author Index 537