

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

Jianying Zhou Moti Yung (Eds.)

Applied Cryptography and Network Security

8th International Conference, ACNS 2010
Beijing, China, June 22-25, 2010
Proceedings

Volume Editors

Jianying Zhou
Institute for Infocomm Research
1 Fusionopolis Way, Singapore, 138632, Singapore
E-mail: jyzhou@i2r.a-star.edu.sg

Moti Yung
Google Inc. and Columbia University
Computer Science Department
New York, NY 10027, USA
E-mail: moti@cs.columbia.edu

Library of Congress Control Number: 2010928335

CR Subject Classification (1998): E.3, E.4, K.6.5, D.4.6, C.2, K.4.4

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN	0302-9743
ISBN-10	3-642-13707-5 Springer Berlin Heidelberg New York
ISBN-13	978-3-642-13707-5 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 2010
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

ACNS 2010, the 8th International Conference on Applied Cryptography and Network Security, was held in Beijing, China, during June 22-25, 2010. ACNS 2010 brought together individuals from academia and industry involved in multiple research disciplines of cryptography and security to foster the exchange of ideas.

ACNS was initiated in 2003, and there has been a steady improvement in the quality of its program over the past 8 years: ACNS 2003 (Kunming, China), ACNS 2004 (Yellow Mountain, China), ACNS 2005 (New York, USA), ACNS 2006 (Singapore), ACNS 2007 (Zhuhai, China), ACNS 2008 (New York, USA), ACNS 2009 (Paris, France). The average acceptance rate has been kept at around 17%, and the average number of participants has been kept at around 100.

The conference received a total of 178 submissions from all over the world. Each submission was assigned to at least three committee members. Submissions co-authored by members of the Program Committee were assigned to at least four committee members. Due to the large number of high-quality submissions, the review process was challenging and we are deeply grateful to the committee members and the external reviewers for their outstanding work. After extensive discussions, the Program Committee selected 32 submissions for presentation in the academic track, and these are the articles that are included in this volume (LNCS 6123). Additionally, a few other submissions were selected for presentation in the non-archival industrial track. The prize for the best student paper was awarded to Mehdi Tibouchi for his paper “On the Broadcast and Validity-Checking Security of PKCS#1 v1.5 Encryption”, co-authored with Aurelie Bauer, Jean-Sebastien Coron, David Naccache, and Damien Vergnaud.

We would like to thank General Chair Yongfei Han and the local organizing team from Beijing University of Technology and ONETS for their efforts in putting this conference together. Our special thanks are due to Ying Qiu for managing the Easy Chair system for paper submission and review. We would also like to thank all the authors who submitted papers and the participants from all over the world who chose to honor us with their attendance.

April 2010

Jianying Zhou
Moti Yung

ACNS 2010

8th International Conference on
Applied Cryptography and Network Security

Beijing, China
June 22–25, 2010

Organized and Sponsored by

Beijing University of Technology & ONETS, China

General Chair

Yongfei Han BJUT & ONETS, China

Program Chairs

Jianying Zhou Institute for Infocomm Research, Singapore
Moti Yung Columbia University & Google, USA

Program Committee

Michel Abdalla	ENS, France
Ben Adida	Harvard University, USA
N. Asokan	Nokia, Finland
Joonsang Baek	I2R, Singapore
Lucas Ballard	Google, USA
Feng Bao	I2R, Singapore
Lujo Bauer	Carnegie Mellon University, USA
Alex Biryukov	Uni. of Luxembourg, Luxembourg
Alexandra Boldyreva	Georgia Tech, USA
Colin Boyd	QUT, Australia
Levente Buttyan	BME, Hungary
Liqun Chen	HP Laboratories, UK
Songqing Chen	George Mason University, USA
Debra Cook	Telcordia, USA
Cas Cremers	ETH Zurich, Switzerland
Sabrina De Capitani di Vimercati	UNIMI, Italy
Robert Deng	SMU, Singapore

VIII Organization

Orr Dunkelman	Weizmann Institute, Israel
Dieter Gollmann	TU Hamburg-Harburg, Germany
Stefanos Gritzalis	University of the Aegean, Greece
Marc Joye	Technicolor, France
Charanjit Jutla	IBM, USA
Angelos Keromytis	Columbia University, USA
Xuejia Lai	Shanghai Jiao Tong University, China
Dong Hoon Lee	Korea University, Korea
Ninghui Li	Purdue University, USA
Yingjiu Li	SMU, Singapore
Benoit Libert	UCL, Belgium
Dongdai Lin	Institute of Software, China
Peng Liu	Pennsylvania State University, USA
Javier Lopez	University of Malaga, Spain
Mark Manulis	TU Darmstadt, Germany
Fabio Martinelli	CNR, Italy
Atefeh Mashatan	EPFL, Switzerland
Paolo Milani	Technical University of Vienna, Austria
Chris Mitchell	RHUL, UK
Atsuko Miyaji	JAIST, Japan
Tatsuaki Okamoto	NTT, Japan
Alina Oprea	RSA Laboratories, USA
Elisabeth Oswald	University of Bristol, UK
Benny Pinkas	University of Haifa, Israel
Pandu Rangan	Indian Institute of Technology, India
Vincent Rijmen	TU Graz, Austria
Mark Ryan	University of Birmingham, UK
Ahmad-Reza Sadeghi	Ruhr-Uni. Bochum, Germany
Reihaneh Safavi-Naini	University of Calgary, Canada
Palash Sarkar	Indian Statistical Institute, India
Nitesh Saxena	Poly Institute of New York Uni., USA
Radu Sion	Stony Brook University, USA
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	FUN, Japan
Duncan Wong	City University of Hong Kong, China

Organizing Chairs

Jian Li	Beijing University of Technology, China
Yu Wang	ONETS, China

Publicity Chairs

Javier Lopez	University of Malaga, Spain
Tsuyoshi Takagi	FUN, Japan
Sijin Li	ONETS, China

Steering Committee

Yongfei Han	BJUT & ONETS, China
Moti Yung	Columbia University & Google, USA
Jianying Zhou	Institute for Infocomm Research, Singapore

External Reviewers

Gergely Acs	Choudary Gorantla	Christoph Ludwig
Isaac Agudo	Tzipora Halevi	Yiyuan Luo
Efthimia Aivaloglou	Christoph Herbst	Hans Lohr
Mansoor Alicherry	Shlomo HersHKop	Ilaria Matteucci
Elli Androulaki	Tamas Holczer	Marcel Medwed
Myrto Arapinis	Qiong Huang	Daisuke Moriyama
Frederik Armknecht	Toshiyuki Isshiki	Andreas Moser
Tomoyuki Asano	Stas Jarecki	Francisco Moyano
Elias Athanasopoulos	Ayman Jarrous	Pablo Najera
Man Ho Au	Seny Kamara	Toru Nakanishi
Jean-Philippe Aumasson	Giorgos Karopoulos	Kris Narayan
Sumeet Bajaj	Vasileios P. Kemerlis	Kris Narayan
Collard Baudoin	Bum Han Kim	Matthias
Bruno Blanchet	Kitak Kim	Neugschwandtner
Marina Blanton	Ilya Kizhvatov	Ching Yu Ng
Shaoying Cai	Miroslav Knezevic	Ivica Nikolic
Tianjie Cao	Clemens Kolbitsch	Geon Tae Noh
Bogdan Carbunar	Deguang Kong	Adam O'Neill
Julien Cathalo	Elisavet Konstantinou	Wakaha Ogata
Sambuddho Chakravarty	Woo Kwon Koo	Katsuyuki Okeya
Shiping Chen	Leanid Krautsevich	Kazumasa Omote
Wei Cheng	Swarun Kumar	Khaled Ouafi
Kyu Young Choi	Virendra Kumar	Carles Padro
Tom Chothia	Francesco la Torre	Jung Ha Paik
Cheng-Kang Chu	Fabien Laguillaumie	Vasilis Pappas
Ji Young Chun	Aliaksandr Lazouski	Sai Tej Peddinti
Gabriele Costa	Hyun Sook Lee	Chris Peikert
Gabriela Cretu	Kwangsue Lee	Kun Peng
Ning Ding	Fagen Li	Christophe Petit
Alexandra Dmitrienko	Tieyan Li	Thomas Plantard
Ming Duan	Wei Li	Bertram Poettering
Mark Felegyhazi	Yan Li	Mariana Raykova
Carmen Fernandez-Gago	Jingqiang Lin	Tzachy Reinman
Dario Fiore	Hanwu Liu	Evangelos Reklitis
Martin Gagne	Joseph. K. Liu	Ruben Rios
Zheng Gong	Mei Cheng Liu	Panagiotis Rizomiliotis
Juan Gonzalez	Xianhui Lu	Rodrigo Roman

Bagus Santoso
 Werner Schindler
 Michael Schneider
 Thomas Schneider
 Dominique Schroder
 Sharmila Deva selvi
 Nicolas Sendrier
 Daniele Sgandurra
 Siamak Shahandashti
 Jun Shao
 Takeshi Shimoyama
 Francesco Sica
 Stelios Sidiroglou
 Matt Smart
 Nigel Smart
 Ben Smyth
 Miroslava Sotakova
 Douglas Stebila
 Thorsten Strufe
 Chunhua Su

Xiaorui Sun
 Martin Szydlowski
 Kouya Tochikubo
 Ashraful Tuhin
 Michael Tunstall
 Berkant Ustaoglu
 Istvan Vajda
 Serge Vaudenay
 Jose Luis Vivas
 Sree Vivek
 Jonathan Voris
 Camille Vuillaume
 Christian Wachsmann
 Zhongmei Wan
 Xinyuan Wang
 Ralf-Philipp Weinmann
 Zhongming Wu
 Fubiao Xia
 Jing Xu
 Guanhua Yan

Qiang Yan
 Guomin Yang
 Artsiom Yautsiukhin
 Kuo-Hui Yeh
 Kazuki Yoneyama
 Junfeng Yu
 Tsz Hon Yuen
 Angelika Zavou
 Bin Zhang
 Min Zhang
 Mingwu Zhang
 Shengzhi Zhang
 Xinwen Zhang
 Yunlei Zhao
 JinMin Zhong
 Chunfang Zhou
 Hong-Sheng Zhou
 Bo Zhu

Table of Contents

Public Key Encryption

On the Broadcast and Validity-Checking Security of PKCS#1 v1.5 Encryption	1
<i>Aur�lie Bauer, Jean-S�bastien Coron, David Naccache, Mehdi Tibouchi, and Damien Vergnaud</i>	
How to Construct Interval Encryption from Binary Tree Encryption	19
<i>Huang Lin, Zhenfu Cao, Xiaohui Liang, Muxin Zhou, Haojin Zhu, and Dongsheng Xing</i>	
Shrinking the Keys of Discrete-Log-Type Lossy Trapdoor Functions	35
<i>Xavier Boyen and Brent Waters</i>	

Digital Signature

Trapdoor Sanitizable Signatures Made Easy	53
<i>Dae Hyun Yum, Jae Woo Seo, and Pil Joong Lee</i>	
Generic Constructions for Verifiably Encrypted Signatures without Random Oracles or NIZKs	69
<i>Markus R�ckert, Michael Schneider, and Dominique Schr�der</i>	
Redactable Signatures for Tree-Structured Data: Definitions and Constructions	87
<i>Christina Brzuska, Heike Busch, Oezguer Dagdelen, Marc Fischlin, Martin Franz, Stefan Katzenbeisser, Mark Manulis, Cristina Onete, Andreas Peter, Bertram Poettering, and Dominique Schr�der</i>	

Block Ciphers and Hash Functions

Impossible Differential Cryptanalysis on Feistel Ciphers with <i>SP</i> and <i>SPS</i> Round Functions	105
<i>Yuechuan Wei, Ping Li, Bing Sun, and Chao Li</i>	
Multi-trail Statistical Saturation Attacks	123
<i>Baudoin Collard and Francois-Xavier Standaert</i>	
Multiset Collision Attacks on Reduced-Round SNOW 3G and SNOW 3G [�]	139
<i>Alex Biryukov, Deike Priemuth-Schmid, and Bin Zhang</i>	
High Performance GHASH Function for Long Messages	154
<i>Nicolas M�loni, Christophe N�gre, and M. Anwar Hasan</i>	

Side-Channel Attacks

Principles on the Security of AES against First and Second-Order Differential Power Analysis	168
<i>Jiqiang Lu, Jing Pan, and Jerry den Hartog</i>	
Adaptive Chosen-Message Side-Channel Attacks	186
<i>Nicolas Veyrat-Charvillon and François-Xavier Standaert</i>	
Secure Multiplicative Masking of Power Functions	200
<i>Laurie Genelle, Emmanuel Prouff, and Michaël Quisquater</i>	

Zero Knowledge and Multi-party Protocols

Batch Groth-Sahai	218
<i>Olivier Blazy, Georg Fuchsbauer, Malika Izabachène, Amandine Jambert, Hervé Sibert, and Damien Vergnaud</i>	
Efficient and Secure Evaluation of Multivariate Polynomials and Applications	236
<i>Matthew Franklin and Payman Mohassel</i>	
Efficient Implementation of the Orlandi Protocol	255
<i>Thomas P. Jakobsen, Marc X. Makkes, and Janus Dam Nielsen</i>	
Improving the Round Complexity of Traitor Tracing Schemes	273
<i>Aggelos Kiayias and Serdar Pehlivanoglu</i>	

Key Management

Password Based Key Exchange Protocols on Elliptic Curves Which Conceal the Public Parameters	291
<i>Julien Bringer, Hervé Chabanne, and Thomas Icart</i>	
Okamoto-Tanaka Revisited: Fully Authenticated Diffie-Hellman with Minimal Overhead	309
<i>Rosario Gennaro, Hugo Krawczyk, and Tal Rabin</i>	
Deniable Internet Key Exchange	329
<i>Andrew C. Yao and Yunlei Zhao</i>	

Authentication and Identification

A New Human Identification Protocol and Coppersmith's Baby-Step Giant-Step Algorithm	349
<i>Hassan Jameel Asghar, Josef Pieprzyk, and Huaxiong Wang</i>	

Secure Sketch for Multiple Secrets	367
<i>Chengfang Fang, Qiming Li, and Ee-Chien Chang</i>	
A Message Recognition Protocol Based on Standard Assumptions	384
<i>Atefeh Mashatan and Serge Vaudenay</i>	

Privacy and Anonymity

Affiliation-Hiding Key Exchange with Untrusted Group Authorities	402
<i>Mark Manulis, Bertram Poettering, and Gene Tsudik</i>	
Privacy-Preserving Group Discovery with Linear Complexity	420
<i>Mark Manulis, Benny Pinkas, and Bertram Poettering</i>	
Two New Efficient PIR-Writing Protocols	438
<i>Helger Lipmaa and Bingsheng Zhang</i>	
Regulatory Compliant Oblivious RAM	456
<i>Bogdan Carbunar and Radu Sion</i>	

RFID Security and Privacy

Revisiting Unpredictability-Based RFID Privacy Models	475
<i>Junzuo Lai, Robert H. Deng, and Yingjiu Li</i>	
On RFID Privacy with Mutual Authentication and Tag Corruption	493
<i>Frederik Armknecht, Ahmad-Reza Sadeghi, Ivan Visconti, and Christian Wachsmann</i>	

Internet Security

Social Network-Based Botnet Command-and-Control: Emerging Threats and Countermeasures	511
<i>Erhan J. Kartaltepe, Jose Andre Morales, Shouhuai Xu, and Ravi Sandhu</i>	
COP: A Step toward Children Online Privacy	529
<i>Wei Xu, Sencun Zhu, and Heng Xu</i>	
A Hybrid Method to Detect Deflation Fraud in Cost-Per-Action Online Advertising	545
<i>Xuhua Ding</i>	
Author Index	563