

Michel Abdalla David Pointcheval
Pierre-Alain Fouque Damien Vergnaud (Eds.)

Applied Cryptography and Network Security

7th International Conference, ACNS 2009
Paris-Rocquencourt, France, June 2-5, 2009
Proceedings

Volume Editors

Michel Abdalla
David Pointcheval
Pierre-Alain Fouque
Damien Vergnaud
École Normale Supérieure
45, rue d'Ulm, 75230 Paris Cedex 05, France
E-mail: {michel.abdalla, david.pointcheval,
pierre-alain.fouque, damien.vergnaud}@ens.fr

Library of Congress Control Number: Applied for

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-01956-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-01956-2 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.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: 12683758 06/3180 5 4 3 2 1 0

Preface

ACNS 2009, the 7th International Conference on Applied Cryptography and Network Security, was held in Paris-Rocquencourt, France, June 2–5, 2009. ACNS 2009 was organized by the École Normale Supérieure (ENS), the French National Center for Scientific Research (CNRS), and the French National Institute for Research in Computer Science and Control (INRIA), in cooperation with the International Association for Cryptologic Research (IACR). The General Chairs of the conference were Pierre-Alain Fouque and Damien Vergnaud.

The conference received 150 submissions and 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 meticulous deliberation, the Program Committee, which was chaired by Michel Abdalla and David Pointcheval, selected 32 submissions for presentation in the academic track and these are the articles that are included in this volume. Additionally, a few other submissions were selected for presentation in the non-archival industrial track. The best student paper was awarded to Ayman Jarrous for his paper “Secure Hamming Distance Based Computation and Its Applications,” co-authored with Benny Pinkas. The review process was run using the iChair software, written by Thomas Baigneres and Matthieu Finiasz from EPFL, LASEC, Switzerland and we are indebted to them for letting us use their software.

The program also included four invited talks in addition to the academic and industrial tracks. The invited talks were given by Craig Gentry from Stanford University on “Fully Homomorphic Encryption Using Ideal Lattices,” Antoine Joux from DGA and the University of Versailles on “Can We Settle Cryptography’s Hash?,” Angelos Keromytis from Columbia University on “Voice Over IP: Risks, Threats and Vulnerabilities,” and Mike Reiter from the University of North Carolina at Chapel Hill on “Better Architectures and New Applications for Coarse Network Monitoring.” We would like to genuinely thank them for accepting our invitation and for contributing to the success of ACNS 2009.

Finally, we would like to thank our sponsors Ingenico, CNRS, and the French National Research Agency (ANR) for their financial support and all the people involved in the organization of this conference. In particular, we would like to thank the Office for Courses and Colloquiums (*Bureau des Cours-Colloques*) from INRIA and Gaëlle Dorkeld for their diligent work and for making this conference possible.

June 2009

Michel Abdalla
David Pointcheval
Pierre-Alain Fouque
Damien Vergnaud

ACNS 2009

7th Annual Conference on
Applied Cryptography and Network Security

Paris-Rocquencourt, France

June 2–5, 2009

Organized by

École Normale Supérieure (ENS)

Centre National de la Recherche Scientifique (CNRS)

Institut National de Recherche en Informatique et en Automatique (INRIA)

In Cooperation with

The International Association for Cryptologic Research (IACR)

General Chairs

Pierre-Alain Fouque

École Normale Supérieure, France

Damien Vergnaud

École Normale Supérieure, France

Program Chairs

Michel Abdalla

École Normale Supérieure, France

David Pointcheval

École Normale Supérieure, France

Program Committee

Gildas Avoine

Université Catholique de Louvain, Belgium

Feng Bao

Institute for Infocomm Research, Singapore

Christophe Bidan

Supélec, France

Alex Biryukov

University of Luxembourg

Xavier Boyen

Stanford University, USA

Dario Catalano

University of Catania, Italy

Liqun Chen

Hewlett Packard Labs, UK

Jean-Sébastien Coron

University of Luxembourg

Jacques Demerjian

CS, France

Aline Gouget

Gemalto, France

Louis Granboulan

EADS, France

Peter Gutmann

University of Auckland, New Zealand

Nick Howgrave-Graham

NTRU Cryptosystems, USA

Stanislaw Jarecki

University of California at Irvine, USA

Marc Joye

Thomson R&D, France

Jaeyeon Jung

Intel, USA

Seny Kamara	Microsoft Research, USA
Jonathan Katz	University of Maryland, USA
Aggelos Kiayias	University of Connecticut, USA
Xuejia Lai	SJTU, China
Javier Lopez	University of Malaga, Spain
Olivier Orcière	Thales, France
Kenny Paterson	Royal Holloway, University of London, UK
Giuseppe Persiano	University of Salerno, Italy
Josef Pieprzyk	University of Macquarie, Australia
Matt Robshaw	Orange Labs, France
Kazue Sako	NEC, Japan
Palash Sarkar	Indian Statistical Institute, India
Berry Schoenmakers	TUE, The Netherlands
Hovav Shacham	University of California at San Diego, USA
Jessica Staddon	PARC, USA
Michael Szydło	Akamai, USA
Serge Vaudenay	EPFL, Switzerland
Avishai Wool	Tel Aviv University, Israel
Duncan Wong	City University of Hong Kong
Jianying Zhou	Institute for Infocomm Research, Singapore

Steering Committee

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

External Reviewers

Asmaa Adnane	Guillaume Fumaroli	Toshiyuki Isshiki
Toshinori Araki	Jun Furukawa	Amandine Jambert
Joonsang Baek	Martin Gagne	Haimin Jin
Aurélie Bauer	Clemente Galdi	Pascal Junod
Bruno Blanchet	David Galindo	Mohamed Karroumi
Carlo Blundo	Benedikt Gierlich	Dmitry Khovratovich
Emmanuel Bresson	Jens Groth	Chung Ki Li
Sébastien Canard	Gilles Guette	Eike Kiltz
Ran Canetti	Sylvain Guilley	Ilya Kizhvatov
Richard Chow	Wei Han	Hugo Krawczyk
Pascal Delaunay	Javier Herranz	Mirosław Kutylowski
Valeria de Paiva	Duong Hieu Phan	Sylvain Lachartre
Mario Di Raimondo	Tsz Hon Yuen	Cédric Lauradoux
Ming Duan	Qiong Huang	David Lefranc
Renaud Dubois	Emeline Hufschmitt	Francois Lesueur
Dario Fiore	Vincenzo Iovino	Tieyan Li

Wei Li	Serdar Pehlivanoglu	Christophe Tartary
Joseph K. Liu	Kun Peng	Isamu Teranishi
Yu Long	Duong Hieu Phan	Frederic Tronel
Xianhui Lu	Gilles Piret	Ivan Visconti
Subhamoy Maitra	Nicolas Prigent	Zhongmai Wan
Krzysztof Majcher	Sasa Radomirovic	Mi Wen
Mark Manulis	Louis Salvail	Jian Weng
Sandra Marcello	Koby Scheuer	Douglas Wikström
Tania Martin	Roman Schlegel	Charles Wright
Krystian Matusiewicz	Yannick Seurin	Hongjun Wu
Petros Mol	Elaine Shi	Yongdong Wu
Jorge Nakahara Jr	Igor Shparlinski	Yaying Xiao
Yossi Oren	Vladimir Shpilrain	Guomin Yang
Khaled Ouafi	Hervé Sibert	Yanjiang Yang
Pascal Paillier	François-Xavier	Yang Yanjiang
Philippe Painchault	Standaert	Bin Zhang
Sylvain Pasini	Ron Steinfeld	Hong-Sheng Zhou
Maura Paterson	Xiaorui Sun	Huafei Zhu

Sponsoring Institutions

Ingenico, Neuilly-sur-Seine, France

The French National Research Agency (ANR), Paris, France

French National Center for Scientific Research (CNRS), Paris, France

Table of Contents

Key Exchange

Group Key Exchange Enabling On-Demand Derivation of Peer-to-Peer Keys	1
<i>Mark Manulis</i>	
Session-state Reveal Is Stronger Than Ephemeral Key Reveal: Attacking the NAXOS Authenticated Key Exchange Protocol	20
<i>Cas J.F. Cremers</i>	
Secure Pairing of “Interface-Constrained” Devices Resistant against Rushing User Behavior	34
<i>Nitesh Saxena and Md. Borhan Uddin</i>	
How to Extract and Expand Randomness: A Summary and Explanation of Existing Results	53
<i>Yvonne Cluff, Colin Boyd, and Juan Gonzalez Nieto</i>	

Secure Computation

Novel Precomputation Schemes for Elliptic Curve Cryptosystems	71
<i>Patrick Longa and Catherine Gebotys</i>	
Practical Secure Evaluation of Semi-private Functions	89
<i>Annika Paus, Ahmad-Reza Sadeghi, and Thomas Schneider</i>	
Secure Hamming Distance Based Computation and Its Applications . . .	107
<i>Ayman Jarrous and Benny Pinkas</i>	
Efficient Robust Private Set Intersection	125
<i>Dana Dachman-Soled, Tal Malkin, Mariana Raykova, and Moti Yung</i>	

Public-Key Encryption

A New Variant of the Cramer-Shoup KEM Secure against Chosen Ciphertext Attack	143
<i>Joosang Baek, Willy Susilo, Joseph K. Liu, and Jianying Zhou</i>	
An Efficient Identity-Based Online/Offline Encryption Scheme	156
<i>Joseph K. Liu and Jianying Zhou</i>	
Dual-Policy Attribute Based Encryption	168
<i>Nuttapong Attrapadung and Hideki Imai</i>	

Construction of Threshold Public-Key Encryptions through Tag-Based Encryptions 186
Seiko Arita and Koji Tsurudome

Network Security I

Malyzer: Defeating Anti-detection for Application-Level Malware Analysis 201
Lei Liu and Songqing Chen

A New Message Recognition Protocol with Self-recoverability for Ad Hoc Pervasive Networks 219
Ian Goldberg, Atefeh Mashatan, and Douglas R. Stinson

Traitor Tracing

Breaking Two k -Resilient Traitor Tracing Schemes with Sublinear Ciphertext Size 238
MoonShik Lee, Daegun Ma, and MinJae Seo

Tracing and Revoking Pirate Rebroadcasts 253
Aggelos Kiayias and Serdar Pehlivanoglu

Authentication and Anonymity

Efficient Deniable Authentication for Signatures: Application to Machine-Readable Travel Document 272
Jean Monnerat, Sylvain Pasini, and Serge Vaudenay

Homomorphic MACs: MAC-Based Integrity for Network Coding 292
Shweta Agrawal and Dan Boneh

Algorithmic Tamper Proof (ATP) Counter Units for Authentication Devices Using PIN 306
Yuichi Komano, Kazuo Ohta, Hideyuki Miyake, and Atsushi Shimbo

Performance Measurements of Tor Hidden Services in Low-Bandwidth Access Networks 324
Jörg Lenhard, Karsten Loesing, and Guido Wirtz

Hash Functions

Cryptanalysis of Twister 342
Florian Mendel, Christian Rechberger, and Martin Schl affer

Cryptanalysis of CubeHash 354
Eric Brier and Thomas Peyrin

Collision Attack on Boole	369
<i>Florian Mendel, Tomislav Nad, and Martin Schl�affer</i>	

Network Security II

Integrity Protection for Revision Control	382
<i>Christian Cachin and Martin Geisler</i>	
Fragility of the Robust Security Network: 802.11 Denial of Service	400
<i>Martin Eian</i>	
Fast Packet Classification Using Condition Factorization	417
<i>Alok Tongaonkar, R. Sekar, and Sreenaath Vasudevan</i>	

Lattices

Choosing NTRUEncrypt Parameters in Light of Combined Lattice Reduction and MITM Approaches	437
<i>Philip S. Hirschhorn, Jeffrey Hoffstein, Nick Howgrave-Graham, and William Whyte</i>	
Broadcast Attacks against Lattice-Based Cryptosystems	456
<i>Thomas Plantard and Willy Susilo</i>	
Partial Key Exposure Attack on CRT-RSA	473
<i>Santanu Sarkar and Subhamoy Maitra</i>	

Side-Channel Attacks

How to Compare Profiled Side-Channel Attacks?	485
<i>Fran�ois-Xavier Standaert, Fran�ois Koeune, and Werner Schindler</i>	
Theoretical and Practical Aspects of Mutual Information Based Side Channel Analysis	499
<i>Emmanuel Prouff and Matthieu Rivain</i>	
Attacking ECDSA-Enabled RFID Devices	519
<i>Michael Hutter, Marcel Medwed, Daniel Hein, and Johannes Wolkerstorfer</i>	

Author Index	535
---------------------------	-----