

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

Kaoru Kurosawa (Ed.)

Advances in Cryptology – ASIACRYPT 2007

13th International Conference on the Theory
and Application of Cryptology and Information Security
Kuching, Malaysia, December 2-6, 2007
Proceedings



Springer

Volume Editor

Kaoru Kurosawa
Ibaraki University
Department of Computer and Information Sciences
4-12-1 Nakanarusawa
Hitachi, Ibaraki 316-8511, Japan
E-mail: kurosawa@mx.ibaraki.ac.jp

Library of Congress Control Number: 2007939450

CR Subject Classification (1998): E.3, D.4.6, F.2.1-2, K.6.5, C.2, J.1, G.2

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-76899-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-76899-9 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 is a part of Springer Science+Business Media

springer.com

©International Association for Cryptology Research 2007
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12194407 06/3180 5 4 3 2 1 0

Preface

ASIACRYPT 2007 was held in Kuching, Sarawak, Malaysia, during December 2–6, 2007. This was the 13th ASIACRYPT conference, and was sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the Information Security Research (iSECURES) Lab of Swinburne University of Technology (Sarawak Campus) and the Sarawak Development Institute (SDI), and was financially supported by the Sarawak Government. The General Chair was Raphael Phan and I had the privilege of serving as the Program Chair.

The conference received 223 submissions (from which one submission was withdrawn). Each paper was reviewed by at least three members of the Program Committee, while submissions co-authored by a Program Committee member were reviewed by at least five members. (Each PC member could submit at most one paper.) Many high-quality papers were submitted, but due to the relatively small number which could be accepted, many very good papers had to be rejected. After 11 weeks of reviewing, the Program Committee selected 33 papers for presentation (two papers were merged). The proceedings contain the revised versions of the accepted papers. These revised papers were not subject to editorial review and the authors bear full responsibility for their contents.

The Committee selected the following two papers as the best papers: “Cryptanalysis of Grindahl” by Thomas Peyrin; and “Faster Addition and Doubling on Elliptic Curves” by Daniel J. Bernstein and Tanja Lange. The authors of these two papers were invited to submit the full version of their paper to the *Journal of Cryptology*. The author of the first paper, Thomas Peyrin, received the Best Paper Award.

The conference featured invited lectures by Ran Canetti and Tatsuaki Okamoto. Ran Canetti’s paper “Treading the Impossible: A Tour of Set-Up Assumptions for Obtaining Universally Composable Security” and Tatsuaki Okamoto’s paper “Authenticated Key Exchange and Key Encapsulation in the Standard Model” have been included in this volume.

There are many people who contributed to the success of ASIACRYPT 2007. I would like to thank many authors from around the world for submitting their papers. I am deeply grateful to the Program Committee for their hard work to ensure that each paper received a thorough and fair review. I gratefully acknowledge the external reviewers listed on the following pages. I am also grateful to Arjen Lenstra, Bart Preneel, and Andy Clark for their advice as the directors of IACR. Finally, I would like to thank the General Chair, Raphael Phan, for organizing the conference and Shai Halevi for developing and maintaining his very nice Web Submission and Review System.

Asiacrypt 2007

December 2–6, 2007, Kuching, Sarawak, Malaysia

Sponsored by
the International Association for Cryptologic Research (IACR)

in cooperation with
the Information Security Research (iSECURES) Lab
of Swinburne University of Technology (Sarawak Campus)

and
the Sarawak Development Institute (SDI)

and
financially supported by the Sarawak Government

General Chair

Raphael C.-W. Phan, EPFL, Switzerland

Program Chair

Kaoru Kurosawa, Ibaraki University, Japan

Program Committee

Masayuki Abe	NTT, Japan
Alex Biryukov	University of Luxembourg, Luxembourg
Alexandra Boldyreva	Georgia Institute of Technology, USA
Jung Hee Cheon	Seoul National University, Korea
Jean-Sebastien Coron	University of Luxembourg, Luxembourg
Joan Daemen	STMicroelectronics, Belgium
Serge Fehr	CWI, Netherlands
Steven Galbraith	Royal Holloway University of London, UK
Craig Gentry	Stanford University, USA
Henri Gilbert	France Telecom, France
Shai Halevi	IBM T.J. Watson Research Center, USA
Helena Handschuh	Spansion, France
Tetsu Iwata	Nagoya University, Japan
Thomas Johansson	Lund University, Sweden
Marc Joye	Thomson R&D France, France
Jonathan Katz	University of Maryland, USA
Lars R. Knudsen	Technical University of Denmark, Denmark

Hugo Krawczyk	IBM T.J. Watson Research Center, USA
Kaoru Kurosawa	Ibaraki University, Japan
Xuejia Lai	Shanghai Jiaotong University, China
Arjen K. Lenstra	EPFL IC LACAL, Switzerland
Stefan Lucks	Bauhaus University Weimar, Germany
Anna Lysyanskaya	Brown University, USA
Alexander May	Technische Universität Darmstadt, Germany
Jesper Buus Nielsen	University of Aarhus, Denmark
Elisabeth Oswald	University of Bristol, UK
Josef Pieprzyk	Macquarie University, Australia
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Pandu Rangan	Indian Institute of Technology, India
Palash Sarkar	Indian Statistical Institute, India
Nigel Smart	Bristol University, UK
Tsuyoshi Takagi	Future University-Hakodate, Japan
Serge Vaudenay	EPFL, Switzerland
Brent Waters	SRI International, USA
Stefan Wolf	ETH Zurich, Switzerland

External Reviewers

Jesus Almansa	Claus Diem	Stuart Haber
Frederik Armknecht	Yevgeniy Dodis	Sang Geun Hahn
Gilles Van Assche	Orr Dunkelman	Safuat Hamdy
Georges Baatz	Håkan Englund	Daewan Han
Thomas Baignères	Pooya Farshim	Wei Han
Boaz Barak	Martin Feldhofer	Goichiro Hanaoka
Mira Belenkiy	Marc Fischlin	Martin Hell
Waldyr Benits	Matthias Fitzi	Dennis Hofheinz
Kamel Bentahar	Ewan Fleischmann	Xuan Hong
Come Berbain	Eiichiro Fujisaki	Nick Howgrave-Graham
Dan Bernstein	Jun Furukawa	Jim Hughes
Guido Bertoni	Philippe Gaborit	Sebastiaan Indesteeghe
Olivier Billet	Nicolas Gama	Tetsuya Izu
Andrey Bogdanov	Pierrick Gaudry	Markus Jakobsson
Arnaud Boscher	Rosario Gennaro	Stas Jarecki
Xavier Boyen	Ralf Gerkmann	Ellen Jochemsz
Ran Canetti	Zheng Gong	Pascal Junod
Christophe De Cannière	Vipul Goyal	Alexandre Karlov
Zhenfu Cao	Rob Granger	Ulrich Kühn
Chris Charnes	Johann Großchädl	Marcelo Kaihara
Sanjit Chatterjee	Gaurav Gupta	Yael Kalai
Scott Contini	Frank Gurkaynak	Alexandre Karlov
Yang Cui	Kil-Chan Ha	Dmitry Khovratovich
Alexander Dent	Robbert de Haan	Eike Kiltz

Vlastimal Klima
 Markulf Kohlweiss
 Yuichi Komano
 Chiu-Yuen Koo
 Ranjit Kumaresan
 Taekyoung Kwon
 Tanja Lange
 Jooyoung Lee
 Mun-Kyu Lee
 Frédéric Lefebvre
 Hoon Wei Lim
 Yehuda Lindell
 Joseph Liu
 Yu Long
 Xianhui Lu
 Changshe Ma
 Subhamoy Maitra
 Keith Martin
 Krystian Matusiewicz
 Florian Mendel
 Daniele Micciancio
 Wil Michiels
 Lorenz Minder
 Andrew Moss
 Siguna Mueller
 Toru Nakanishi
 Arvind Narayanan
 Gregory Neven
 Phong Nguyen
 Svetla Nikova
 Ryo Nishimaki
 Adam O'Neill
 Miyako Ohkubo
 Katsuyuki Okeya

Dag Arne Osvik
 Khaled Ouafi
 Dan Page
 Pascal Paillier
 Sylvain Pasini
 Rafael Pass
 Vijayakrishnan
 Pasupathinathan
 Kenny Paterson
 Maura Paterson
 Thomas Peyrin
 Duong Hieu Phan
 Krzysztof Pietrzak
 Norbert Pramstaller
 Deike Priemuth-Schmid
 Prashant Punya
 Wenfeng Qi
 Tal Rabin
 Dominik Raub
 Christian Rechberger
 Tom Ristenpart
 Maike Ritzenhofen
 Matthieu Rivain
 Panagiotis Rizomiliotis
 Matthew Robshaw
 Kazuo Sakiyama
 Joern-Marc Schmidt
 Yannick Seurin
 Runting Shi
 Masaaki Shirase
 Igor Shparlinski
 Tom Shrimpton
 Ben Smith
 Martijn Stam

Ron Steinfeld
 Marc Stevens
 Koutarou Suzuki
 Christophe Tartary
 Emin Islam Tatli
 Isamu Teranishi
 Soren Thomsen
 Stefan Tillich
 Frederik Vercauteren
 Martin Vuagnoux
 Camille Vuillaume
 Zhongmei Wan
 Huaxiong Wang
 Bogdan Warinschi
 Hoeteck Wee
 Benne de Weger
 Ralf-Philipp Weinmann
 Mi Wen
 William Whyte
 Christopher Wolf
 Duncan Wong
 Hongjun Wu
 Juerg Wullschlegler
 Go Yamamoto
 Bo-Yin Yang
 Jin Yuan
 Aaram Yun
 Erik Zenner
 Xianmo Zhang
 Yunlei Zhao
 Jinmin Zhong

Table of Contents

Number Theory and Elliptic Curve

A Kilobit Special Number Field Sieve Factorization	1
<i>Kazumaro Aoki, Jens Franke, Thorsten Kleinjung, Arjen K. Lenstra, and Dag Arne Osvik</i>	
When e -th Roots Become Easier Than Factoring	13
<i>Antoine Joux, David Naccache, and Emmanuel Thomé</i>	
Faster Addition and Doubling on Elliptic Curves	29
<i>Daniel J. Bernstein and Tanja Lange</i>	

Protocol

A Non-interactive Shuffle with Pairing Based Verifiability	51
<i>Jens Groth and Steve Lu</i>	
On Privacy Models for RFID	68
<i>Serge Vaudenay</i>	

Invited Talk I

Obtaining Universally Composable Security: Towards the Bare Bones of Trust	88
<i>Ran Canetti</i>	

Hash Function Design

A Simple Variant of the Merkle-Damgård Scheme with a Permutation	113
<i>Shoichi Hirose, Je Hong Park, and Aaram Yun</i>	
Seven-Property-Preserving Iterated Hashing: ROX	130
<i>Elena Andreeva, Gregory Neven, Bart Preneel, and Thomas Shrimpton</i>	
How to Build a Hash Function from Any Collision-Resistant Function	147
<i>Thomas Ristenpart and Thomas Shrimpton</i>	

Group/Broadcast Cryptography

Fully Anonymous Group Signatures Without Random Oracles	164
<i>Jens Groth</i>	

Group Encryption	181
<i>Aggelos Kiayias, Yiannis Tsiounis, and Moti Yung</i>	

Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys	200
<i>Cécile Delerablée</i>	

MAC and Implementation

Boosting Merkle-Damgård Hashing for Message Authentication	216
<i>Kan Yasuda</i>	

On Efficient Message Authentication Via Block Cipher Design Techniques	232
<i>G. Jakimoski and K.P. Subbalakshmi</i>	

Symmetric Key Cryptography on Modern Graphics Hardware	249
<i>Jason Yang and James Goodman</i>	

Multiparty Computation I

Blind Identity-Based Encryption and Simulatable Oblivious Transfer . . .	265
<i>Matthew Green and Susan Hohenberger</i>	

Multi-party Indirect Indexing and Applications	283
<i>Matthew Franklin, Mark Gondree, and Payman Mohassel</i>	

Two-Party Computing with Encrypted Data	298
<i>Seung Geol Choi, Ariel Elbaz, Ari Juels, Tal Malkin, and Moti Yung</i>	

Block Ciphers

Known-Key Distinguishers for Some Block Ciphers	315
<i>Lars R. Knudsen and Vincent Rijmen</i>	

Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions	325
<i>Jacques Patarin, Valérie Nachez, and Côme Berbain</i>	

On Tweaking Luby-Rackoff Blockciphers	342
<i>David Goldenberg, Susan Hohenberger, Moses Liskov, Elizabeth Crump Schwartz, and Hakan Seyalioglu</i>	

Multiparty Computation II

Secure Protocols with Asymmetric Trust	357
<i>Ivan Damgård, Yvo Desmedt, Matthias Fitzi, and Jesper Buus Nielsen</i>	

Simple and Efficient Perfectly-Secure Asynchronous MPC	376
<i>Zuzana Beerliová-Trubíniová and Martin Hirt</i>	
Efficient Byzantine Agreement with Faulty Minority	393
<i>Zuzana Beerliová-Trubíniová, Martin Hirt, and Micha Riser</i>	
Information-Theoretic Security Without an Honest Majority	410
<i>Anne Broadbent and Alain Tapp</i>	

Foundation

Black-Box Extension Fields and the Inexistence of Field-Homomorphic One-Way Permutations	427
<i>Ueli Maurer and Dominik Raub</i>	
Concurrent Statistical Zero-Knowledge Arguments for NP from One Way Functions	444
<i>Vipul Goyal, Ryan Moriarty, Rafail Ostrovsky, and Amit Sahai</i>	
Anonymous Quantum Communication	460
<i>Gilles Brassard, Anne Broadbent, Joseph Fitzsimons, Sébastien Gambs, and Alain Tapp</i>	

Invited Talk II

Authenticated Key Exchange and Key Encapsulation in the Standard Model	474
<i>Tatsuaki Okamoto</i>	

Public Key Encryption

Miniature CCA2 PK Encryption: Tight Security Without Redundancy	485
<i>Xavier Boyen</i>	
Bounded CCA2-Secure Encryption	502
<i>Ronald Cramer, Goichiro Hanaoka, Dennis Hofheinz, Hideki Imai, Eike Kiltz, Rafael Pass, Abhi Shelat, and Vinod Vaikuntanathan</i>	
Relations Among Notions of Non-malleability for Encryption	519
<i>Rafael Pass, Abhi Shelat, and Vinod Vaikuntanathan</i>	

Cryptanalysis

Cryptanalysis of the Tiger Hash Function	536
<i>Florian Mendel and Vincent Rijmen</i>	
Cryptanalysis of GRINDAHL	551
<i>Thomas Peyrin</i>	

A Key Recovery Attack on Edon80 568
 Martin Hell and Thomas Johansson

Author Index 583