Lecture Notes in Computer Science 6632

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Kenneth G. Paterson (Ed.)

Advances in Cryptology – EUROCRYPT 2011

30th Annual International Conference
on the Theory and Applications of Cryptographic Techniques
Tallinn, Estonia, May 15-19, 2011
Proceedings

Springer

Volume Editor

Kenneth G. Paterson
Information Security Group (ISG)
Royal Holloway
University of London
Egham, Surrey TW20 0EX, UK
E-mail: kenny.paterson@rhul.ac.uk

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-20464-7 e-ISBN 978-3-642-20465-4
DOI 10.1007/978-3-642-20465-4
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011924899

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

LNCS Sublibrary: SL 4 – Security and Cryptology

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

These are the proceedings of Eurocrypt 2011, the 30th in the series of European Conferences on the Theory and Applications of Cryptographic Techniques. The conference was organized under the auspices of the International Association for Cryptologic Research and was held in Tallinn, Estonia, during May 15–19, 2011.

The aim of this series of conferences is to bring together leading researchers and practitioners from academia and industry in the field of cryptography. The conference program is intended to reflect the best of cryptographic research, in its widest sense. This year, a deliberate attempt was made to broaden the technical scope of the conference without making any compromise to its quality. The main mechanism for achieving this was to select Program Committee members from as broad a range of sub-areas of the field as possible, with the intention of sending a clear signal to potential authors from the field as a whole. I trust that readers of this volume find plenty to interest them here, and agree that the quality of the papers is as high as ever.

The program consisted of 2 invited talks and 31 contributed papers. The invited speakers were Ronald Cramer (CWI, Amsterdam and Mathematical Institute, Leiden) and Phong Nguyen (INRIA and ENS). I would like to thank them for accepting my invitation, for supplying informative abstracts for these proceedings, and for delivering excellent talks. It was a privilege to have such luminaries of our field as invited speakers.

The contributed papers were selected from 167 submissions. Each paper was reviewed by at least three people, with the submissions involving Program Committee members being subjected to at least five reviews each. There was significant online discussion about many of the papers, and a full-day Program Committee meeting was held at Royal Holloway on January 12, 2011 to finalize the program. The Program Committee decided to make a best paper award this year, and the award went to Eike Kiltz, Krzysztof Pietrzak, David Cash, Abhishek Jain and Daniele Venturi for their paper "Efficient Authentication from Hard Learning Problems".

I would like to thank all the people who helped with the conference program and organization, particularly the General Chair, Helger Lipmaa. My heartfelt thanks go to the Program Committee and their sub-reviewers, as listed on the following pages, for their thoroughness during the review process. We had a tough assignment with many submissions and tight deadlines, and the committee members acted with utmost professionalism and attention to detail throughout. My particular thanks are due to Henri Gilbert, the previous Program Chair, who shared many insights with me, and to David Pointcheval, the next Program Chair, who kindly agreed to join the committee at short notice and who acted as a very effective "sweeper."

The submission and review process was greatly simplified by the ichair software developed by Thomas Baignères and Matthieu Finiasz. My thanks to them for producing this software and helping me with some technical queries during the review process. I will be sending them some Estonian delicacies by way of thanks; I highly recommend their software to all future Program Chairs. Thanks are also due to Tristan Findley and Jon Hart at Royal Holloway for maintaining the submission server and for their IT support during the Program Committee meeting.

I am grateful to the authors of all submitted papers for supporting the conference. The authors of accepted papers are thanked again for revising their papers according to the suggestions of the reviewers and for returning latex source files in good time. The revised versions were not checked by the Program Committee so authors bear full responsibility for their contents. I thank the staff at Springer for their help with producing the proceedings.

EuroCrypt 2011 was supported by the European Regional Development Fund (ERDF) through the Estonian Centre of Excellence in Computer Science, EXCS. I would also like to thank Guardtime, Qualcomm and Swedbank, the other sponsors of EuroCrypt 2011, for their generous support.

Finally, I would like to thank my partner Liz and my daughter Cara for their forbearance during a particularly hectic period.

February 2011 Kenny Paterson

Organization

Program Chair

Kenny Paterson	Royal Holloway, University of London, UK

General Chairs

Helger Lipmaa	Cybernetica AS, Estonia and Tallinn University, Estonia

Sponsors

The European Regional Development Fund (ERDF)
Guardtime
Qualcomm
Swedbank

Program Committee

Michel Abdalla	ENS Paris, France
Dan Bernstein	University of Chicago, USA
Xavier Boyen	University of Liege, Belgium
Christian Cachin	IBM Research, Switzerland
Orr Dunkelman	Weizmann Institute of Science, Israel
Pierrick Gaudry	LORIA, France
Henri Gilbert (2010 PC chair)	ANSSI, France
Jonathan Katz	University of Maryland, USA
Yoshi Kohno	University of Washington, USA
Benoit Libert	UCL, Belgium
Anna Lysyanskaya	Brown University, USA
Vadim Lyubashevsky	ENS Paris, France
Alex May	Ruhr University Bochum, Germany
Alfred Menezes	University of Waterloo, Canada
Tatsuaki Okamoto	NTT Labs, Japan
Rafail Ostrovsky	UCLA, USA
Elisabeth Oswald	University of Bristol, UK
Christof Paar	Ruhr University Bochum, Germany
Kenny Paterson (PC chair)	Royal Holloway, University of London, UK
Chris Peikert	Georgia Tech, USA
David Pointcheval (2012 PC chair)	ENS Paris, France

Renato Renner	ETH Zürich, Switzerland
Vincent Rijmen	K.U. Leuven, Belgium and TU Graz, Austria
Berry Schoenmakers	TU Eindhoven, The Netherlands
Mike Scott	DCU, Ireland
Hovav Shacham	UCSD, USA
Thomas Shrimpton	Portland State University, USA
Martijn Stam	EPFL, Switzerland
Doug Stinson	University of Waterloo, Canada
Frederik Vercauteren	K.U. Leuven, Belgium

Sub-reviewers

Johan Aaberg
Masayuki Abe
Divesh Aggarwal
Carlos Aguilar Melchor
Elena Andreeva
Benny Applebaum
Abhishek Banerjee
Aurelie Bauer
Georg Becker
Gaetan Bisson
Andrey Bogdanov
Joppe Bos
Zvika Brakerski
Christina Brzuska
Jan Camenisch
David Cash
Dario Catalano
Nishanth Chandran
Melissa Chase
Sanjit Chatterjee
Céline Chevalier
Sherman Chow
Jeremy Clark
Baudoin Collard
Daniel Dadush
Jean Paul Degabriele
Alex Dent
Claus Diem
Marten van Dijk
Dejan Dukaric
Frederic Dupuis
Thomas Eisenbarth
Nicolas Estibals
Junfeng Fan
Pooya Farshim
Sebastian Faust
Serge Fehr
Matthieu Finiasz
Dario Fiore
Marc Fischlin
Thomas Fuhr
Philippe Gaborit
Steven Galbraith
Sanjam Garg
Praveen Gauravaram
Ran Gelles
Clint Givens
Dov Gordon
Robert Granger
Jens Groth
Esther Haenggi
Brett Hemenway
Jens Hermans
Mathias Herrmann
Florian Hess
Stefan Heyse
Dennis Hofheinz
Susan Hohenberger
S.J.A. de Hoogh
Sebastiaan Indesteege
Abhishek Jain
Antoine Joux
Yael Tauman Kalai
Koray Karabina
Timo Kasper
Aniket Kate
Eike Kiltz
Mehmet S. Kiraz
Mikkel Krigrd
A. Kumarasubramanian
Mario Lamberger
Tanja Lange
Gregor Leander
Anja Lehmann
Arjen K. Lenstra
Peter van Liesdonk
Richard Lindner
Mark Manulis
Bart Mennink
Alexander Meurer
Petros Mol
Amir Moradi
Sean Murphy
Toru Nakanishi
Gregory Neven
Phong Nguyen
Jesper Buus Nielsen
Svetla Nikova
Ryo Nishimaki
Mehrdad Nojoumian
Femi Olumofin
Adam O'Neill
Onur Özen
Carles Padro
Rafael Pass
Ludovic Perret
Thomas Peters
Duong Hieu Phan
Krzysztof Pietrzak

Pandu Rangan
Oded Regev
Leo Reyzin
Alfredo Rial
Thomas Ristenpart
Matthieu Rivain
Louis Salvail
Rüdiger Schack
Christian Schaffner
Martin Schläffer
Aaron Segal
Yannick Seurin
Hakan Seyaliog
Aydin Sezgin
abhi shelat
Francesco Sica
Joe Silverman
Nigel Smart
F.-X. Standaert
Damien Stehlé
Anton Stolbunov
Björn Tackmann
Katsuyuki Takashima
Stefano Tessaro
Enrico Thomae
Deniz Toz
Joana Treger
Dominique Unruh
Vinod Vaikuntanathan
Kerem Varici
Damien Vergnaud
Marion Videau
Jorge L. Villar
Ivan Visconti
Akshay Wadia
Bogdan Warinschi
Brent Waters
Gaven Watson
Severin Winkler
Christopher Wolf
Stefan Wolf
Jiang Wu
Jürg Wullschleger
Keita Xagawa
Go Yamamoto
Kan Yasuda
Ralf Zimmermann

Table of Contents

Invited Talks

The Arithmetic Codex: Theory and Applications (Abstract) 1
Ronald Cramer

Lattice Reduction Algorithms: Theory and Practice 2
Phong Q. Nguyen

Lattice-Based Cryptography

Efficient Authentication from Hard Learning Problems 7
Eike Kiltz, Krzysztof Pietrzak, David Cash, Abhishek Jain, and Daniele Venturi

Making NTRU as Secure as Worst-Case Problems over Ideal Lattices 27
Damien Stehlé and Ron Steinfeld

Implementation and Side Channels

Faster Explicit Formulas for Computing Pairings over Ordinary Curves 48
Diego F. Aranha, Koray Karabina, Patrick Longa, Catherine H. Gebotys, and Julio López

Pushing the Limits: A Very Compact and a Threshold Implementation of AES 69
Amir Moradi, Axel Poschmann, San Ling, Christof Paar, and Huaxiong Wang

Fully Leakage-Resilient Signatures 89
Elette Boyle, Gil Segev, and Daniel Wichs

A Formal Study of Power Variability Issues and Side-Channel Attacks for Nanoscale Devices 109
Mathieu Renauld, François-Xavier Standaert, Nicolas Veyrat-Charvillon, Dina Kamel, and Denis Flandre

Homomorphic Cryptography

Implementing Gentry's Fully-Homomorphic Encryption Scheme 129
Craig Gentry and Shai Halevi

Homomorphic Signatures for Polynomial Functions 149
Dan Boneh and David Mandell Freeman

Semi-homomorphic Encryption and Multiparty Computation 169
Rikke Bendlin, Ivan Damgård, Claudio Orlandi, and Sarah Zakarias

Signature Schemes

Tight Proofs for Signature Schemes without Random Oracles 189
Sven Schäge

Adaptive Pseudo-free Groups and Applications 207
Dario Catalano, Dario Fiore, and Bogdan Warinschi

Commuting Signatures and Verifiable Encryption 224
Georg Fuchsbauer

Information-Theoretic Cryptography

Secure Authentication from a Weak Key, without Leaking Information 246
Niek J. Bouman and Serge Fehr

Secret Keys from Channel Noise 266
Hadi Ahmadi and Reihaneh Safavi-Naini

Almost Optimum t-Cheater Identifiable Secret Sharing Schemes 284
Satoshi Obana

Symmetric Key Cryptography

On Linear Hulls, Statistical Saturation Attacks, PRESENT and a Cryptanalysis of PUFFIN 303
Gregor Leander

Domain Extension for MACs Beyond the Birthday Barrier 323
Yevgeniy Dodis and John Steinberger

Attacks and Algorithms

Statistical Attack on RC4: Distinguishing WPA 343
Pouyan Sepehrdad, Serge Vaudenay, and Martin Vuagnoux

Improved Generic Algorithms for Hard Knapsacks 364
Anja Becker, Jean-Sébastien Coron, and Antoine Joux

Secure Computation

Two-Output Secure Computation with Malicious Adversaries 386
Abhi Shelat and Chih-Hao Shen

Efficient Non-interactive Secure Computation 406
Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, and Amit Sahai

Towards a Game Theoretic View of Secure Computation 426
Gilad Asharov, Ran Canetti, and Carmit Hazay

Highly-Efficient Universally-Composable Commitments Based on the DDH Assumption 446
Yehuda Lindell

Composability

Concurrent Composition in the Bounded Quantum Storage Model 467
Dominique Unruh

Careful with Composition: Limitations of the Indifferentiability Framework 487
Thomas Ristenpart, Hovav Shacham, and Thomas Shrimpton

Key Dependent Message Security

Efficient Circuit-Size Independent Public Key Encryption with KDM Security 507
Tal Malkin, Isamu Teranishi, and Moti Yung

Key-Dependent Message Security: Generic Amplification and Completeness 527
Benny Applebaum

Public Key Encryption

Unbounded HIBE and Attribute-Based Encryption 547
Allison Lewko and Brent Waters

Decentralizing Attribute-Based Encryption 568
Allison Lewko and Brent Waters

Threshold and Revocation Cryptosystems via Extractable Hash Proofs 589
Hoeteck Wee

Deniable Encryption with Negligible Detection Probability: An Interactive Construction 610
Markus Dürmuth and David Mandell Freeman

Author Index 627