

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 for Informatics, Saarbruecken, Germany

Bo-Yin Yang (Ed.)

Post-Quantum Cryptography

4th International Workshop, PQCrypto 2011
Taipei, Taiwan, November 29 – December 2, 2011
Proceedings

Volume Editor

Bo-Yin Yang
Academia Sinica
Institute of Information Science
128 Section 2 Academia Road, Taipei 115, Taiwan
E-mail: by@moscito.org

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-25404-8 e-ISBN 978-3-642-25405-5
DOI 10.1007/978-3-642-25405-5
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011940842

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

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2011

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

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)

Foreword

With Shor's algorithm (Peter W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", *SIAM J. Sci. Statist. Comput.* 41 (2): 303–332, 1999) and its first public instantiation in 2001, when Isaac Chuang and Neil Gershenfeld implemented Shor's algorithm on a 7-qubit quantum computer, it became common knowledge that RSA will crumble with the advent of large quantum computers. Follow-ups made it clear that discrete logarithm problems are equally as broken when thousands-of-qubits quantum computing became available.

A decade had passed and large quantum computers did not actually appear, but it seemed clear enough that the cryptographic research community should not await ostrich-like for the first public appearance of quantum computing to look for alternatives to RSA.

It was in this atmosphere that we saw the emergence, and in some cases renaissance, of "alternative" approaches to public-key cryptography that would survive quantum computers, for which the term "post-quantum cryptography" was affectionately coined.

Cryptographers were hard at work looking for new possibilities for public-key cryptosystems that could resist quantum computers, and currently there are four major families of post-quantum public-key cryptosystems: the code-based public-key cryptosystems, the hash-based public-key cryptosystems, the lattice-based public-key cryptosystems and the multivariate public-key cryptosystems. Many possibilities were proposed and quite a few were rejected. With the increase of research activity in post-quantum cryptography, it became clear that a venue is needed where ideas can be exchanged, results can be presented, and the newest developments can be made known to the world.

Thus was born the first Post-Quantum Cryptography, or PQCrypto, workshop in May 2006 in Leuven. This workshop did not have formal proceedings, and was only made possible with support of the European Union's Framework Program project ECRYPT. PQCrypto 2006 was such a success, however, that Post-Quantum Cryptography was encouraged to form a Steering Committee and run two more instances of these workshop in 2008 (October in Cincinnati, USA) and 2010 (May in Darmstadt, Germany).

The fourth event of this series, PQCrypto 2011, was organized in Taipei, Taiwan, by the Department of Electrical Engineering at the National Taiwan University during November 29–December 2, 2011. The Program Committee received 38 proposals of contributed talks from which 18 were selected. Each paper was thoroughly examined by several independent experts from the Program Committee and additional external reviewers. The papers along with the reviews were then scrutinized by the Program Committee members during a discussion phase after which recommendations were given to all authors. In several

cases, we required the authors to work with a shepherd to ensure that the text was edited in accordance with the committee comments and a high standard of writing. Revised versions of the accepted contributions are published in these proceedings.

Thanks must go to all authors for submitting their quality research work to the conference. Even more deserving are the Program Committee and our external reviewers for their time and energy to ensure that a conference program and a volume of high scientific quality could be assembled.

I thank my fellow organizers: Chen-Mou Cheng, who made all the worldly arrangements, and Peter Schwabe, our capable indefatigable webmaster. We would also like to thank Springer, in particular Alfred Hofmann and Anna Kramer, for their support in publishing these proceedings.

September 2011

Bo-Yin Yang

Organization

PQCrypto 2011 was organized by the Department of Electrical Engineering at the National Taiwan University, Taipei, Taiwan; we thank Intel, the National Science Council of Taiwan, and Academia Sinica for sponsorship.

General Chair

Chen-Mou (Doug) Cheng

National Taiwan University, Taiwan

Program Chair

Bo-Yin Yang

Academia Sinica, Taiwan

Program Committee

Martin R. Albrecht	Université Pierre et Marie Curie, France
Paulo S.L.M. Barreto	Universidade de São Paulo, Brazil
Daniel J. Bernstein	University of Illinois at Chicago, USA
Johannes A. Buchmann	Technische Universität Darmstadt, Germany
Jintai Ding	University of Cincinnati, USA
Vivien Dubois	Direction générale de l'armement, France
Louis Goubin	Université de Versailles, France
Sean Hallgren	Pennsylvania State University, USA
Lars Knudsen	Danmarks Tekniske Universitet, Denmark
Tanja Lange	Technische Universiteit Eindhoven, The Netherlands
Richard Lindner	Technische Universität Darmstadt, Germany
Vadim Lyubashevsky	École Normale Supérieure Paris, France
Daniele Micciancio	University of California at San Diego, USA
Michele Mosca	University of Waterloo, Canada
Chris Peikert	Georgia Institute of Technology, USA
Christiane Peters	Technische Universiteit Eindhoven, The Netherlands
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Nicolas Sendrier	INRIA Paris-Rocquencourt, France
Damien Stehlé	CNRS and École Normale Supérieure de Lyon, France
Jean-Pierre Tillich	INRIA Paris-Rocquencourt, France
Ralf-Philipp Weinmann	Université du Luxembourg, Luxembourg
Christopher Wolf	Ruhr-Universität Bochum, Germany

Webmaster

Peter Schwabe

National Taiwan University, Taiwan

External Reviewers

Romain Alleaume

Thierry Berger

Gaëtan Bisson

Stanislav Bulygin

Jean-Marc Couveignes

Christina Delfs

Kirsten Eisenträger

Pooya Farshim

Thomas Feller

Matthieu Finiasz

Philippe Gaborit

Steven Galbraith

Nicolas Gama

Ryan Henry

Jens Hermans

Stefan Heyse

Gerhard Hoffmann

Jeff Hoffstein

Andreas Hülsing

Po-Chun Kuo

Feng-Hao Liu

Pierre Loidreau

Alexander Meurer

Rafael Misoczki

Petros Mol

Michael Naehrig

Robert Niebuhr

Jacques Patarin

Kenny Paterson

Ludovic Perret

Edoardo Persichetti

Albrecht Petzoldt

Louis Salvail

Michael Schneider

Julien Schrek

Jieh-Ren Jarron Shih

Boris Skorik

Benjamin Smith

Douglas Stebila

Andreas Stein

Ron Steinfeld

Enrico Thomae

Valerie Gauthier Umana

Frederik Vercauteren

William Whyte

PQCrypto Steering Committee

Dan Bernstein

Johannes Buchmann

Claude Crépeau

Jintai Ding

Philippe Gaborit

Tanja Lange

University of Illinois at Chicago, USA

Technische Universität Darmstadt, Germany

McGill University, Canada

University of Cincinnati, USA

Université de Limoges, France

Technische Universiteit Eindhoven,
The Netherlands

Daniele Micciancio

Werner Schindler

Nicolas Sendrier

Shigeo Tsujii

Bo-Yin Yang

University of California at San Diego, USA

BSI, Germany

INRIA, France

Chuo University, Japan

Academia Sinica, Taiwan

Sponsoring Institutions

Institute of Information Science, Academia Sinica

Center of Information Technology and Innovation, Academia Sinica

The Intel Connected Context Computing Center (at National Taiwan University)

Table of Contents

General Fault Attacks on Multivariate Public Key Cryptosystems	1
<i>Yasufumi Hashimoto, Tsuyoshi Takagi, and Kouichi Sakurai</i>	
Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies	19
<i>David Jao and Luca De Feo</i>	
Full Cryptanalysis of the Chen Identification Protocol	35
<i>Philippe Gaborit, Julien Schrek, and Gilles Zémor</i>	
Decoding One Out of Many	51
<i>Nicolas Sendrier</i>	
On Provable Security of UOV and HFE Signature Schemes against Chosen-Message Attack	68
<i>Koichi Sakumoto, Taizo Shirai, and Harunaga Hiwatari</i>	
Roots of Square: Cryptanalysis of Double-Layer Square and Square+ . . .	83
<i>Enrico Thomae and Christopher Wolf</i>	
An Efficient Attack on All Concrete KKS Proposals	98
<i>Ayoub Otmani and Jean-Pierre Tillich</i>	
XMSS – A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions	117
<i>Johannes Buchmann, Erik Dahmen, and Andreas Hülsing</i>	
On the Differential Security of Multivariate Public Key Cryptosystems	130
<i>Daniel Smith-Tone</i>	
Implementation of McEliece Based on Quasi-dyadic Goppa Codes for Embedded Devices	143
<i>Stefan Heyse</i>	
Efficient Threshold Encryption from Lossy Trapdoor Functions	163
<i>Xiang Xie, Rui Xue, and Rui Zhang</i>	
Monoidic Codes in Cryptography	179
<i>Paulo S.L.M. Barreto, Richard Lindner, and Rafael Misoczki</i>	
Simplified High-Speed High-Distance List Decoding for Alternant Codes	200
<i>Daniel J. Bernstein</i>	

Statistical Decoding of Codes over \mathbb{F}_q	217
<i>Robert Niebuhr</i>	
High-Speed Hardware Implementation of Rainbow Signature on FPGAs	228
<i>Shaohua Tang, Haibo Yi, Jintai Ding, Huan Chen, and Guomin Chen</i>	
Wild McEliece Incognito	244
<i>Daniel J. Bernstein, Tanja Lange, and Christiane Peters</i>	
A New Spin on Quantum Cryptography: Avoiding Trapdoors and Embracing Public Keys	255
<i>Lawrence M. Ioannou and Michele Mosca</i>	
A Security Analysis of Uniformly-Layered Rainbow: Revisiting Sato-Araki's Non-commutative Approach to Ong-Schnorr-Shamir Signature towards PostQuantum Paradigm	275
<i>Takanori Yasuda and Kouichi Sakurai</i>	
Author Index	295