Lecture Notes in Computer Science 7071

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

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

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 Skoric
Benjamin Smith
Douglas Stebila
Andreas Stein
Ron Steinfeld
Enrico Thomae
Valerie Gauthier Umana
Frederik Vercauteren
William Whyte

PQCrypto Steering Committee

Dan Bernstein	University of Illinois at Chicago, USA
Johannes Buchmann	Technische Universität Darmstadt, Germany
Claude Crépeau	McGill University, Canada
Jintai Ding	University of Cincinnati, USA
Philippe Gaborit	Université de Limoges, France
Tanja Lange	Technische Universiteit Eindhoven, The Netherlands
Daniele Micciancio	University of California at San Diego, USA
Werner Schindler	BSI, Germany
Nicolas Sendrier	INRIA, France
Shigeo Tsujii	Chuo University, Japan
Bo-Yin Yang	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