Lecture Notes in Computer Science 8772

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

Michele Mosca (Ed.)

Post-Quantum Cryptography

6th International Workshop, PQCrypto 2014
Waterloo, ON, Canada, October 1-3, 2014
Proceedings

Volume Editor

Michele Mosca
University of Waterloo
Institute for Quantum Computing
200 University Avenue West
Waterloo, ON N2L 3G1, Canada
E-mail: mmosca@uwaterloo.ca

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-319-11658-7 e-ISBN 978-3-319-11659-4
DOI 10.1007/978-3-319-11659-4
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014948669

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

PQCrypto 2014, the 6th International Workshop on Post-Quantum Cryptography was held in Waterloo, Ontario, Canada, during 1–3 October 2014.

On the 20th anniversary of Shor's algorithms for breaking factoring and discrete log based cryptosystems, there is a new landscape of quantum tools and intensifying efforts worldwide to build large-scale quantum computers. The aim of PQCrypto is to serve as a forum for researchers to present results and exchange ideas on the topic of cryptography in an era with large-scale quantum computers. The workshop was preceded by a summer school from 29–30 September 2014.

The workshop attracted 37 submissions, of which the Program Committee selected 16 for publication in the workshop proceedings. The accepted papers dealt with the topics of code-based cryptography, lattice-based cryptography, multivariate-cryptography, isogeny-based cryptography, security proof frameworks, cryptanalysis, and implementations. The Program Committee included 26 subject-matter experts from 10 countries.

The workshop included four invited talks by Lily Chen (NIST), Nicolas Gisin (Université de Genève), Matteo Mariantoni (University of Waterloo), and Vinod Vaikuntanathan (MIT), tours of the experimental facilities at the Institute for Quantum Computing, and a recent results session.

I am very grateful to all the Program Committee members for generously contributing their time, knowledge and expertise. Many thanks also to the external reviewers who assisted in the process.

I wish to thank the generous sponsors and partners of PQCrypto 2014 who made it possible to host this event and support the invited speakers and other participants.

Profound thanks are also due to Alfred Menezes for his organizational effort and general guidance as the general chair and to Kim Simmermaker and the Institute for Quantum Computing staff for their logistical support.

July 2014 Michele Mosca

Organization

General Chair

Alfred Menezes	University of Waterloo, Canada

Program Chair

Michele Mosca	University of Waterloo, Canada

Steering Committee

Daniel J. Bernstein	University of Illinois at Chicago, USA and Technische Universiteit Eindhoven, The Netherlands
Johannes Buchmann	Technische Universität Darmstadt, Germany
Claude Crépeau	McGill University, Canada
Jintai Ding	University of Cincinnati, USA
Philippe Gaborit	University of Limoges, France
Tanja Lange	Technische Universiteit Eindhoven, The Netherlands
Daniele Micciancio	University of California at San Diego, USA
Michele Mosca	University of Waterloo, Canada
Nicolas Sendrier	Inria, France
Shigeo Tsujii	Chuo University, Japan
Bo-Yin Yang	Academia Sinica, Taiwan

Program Committee

Paulo Barreto	University of São Paulo, Brazil
Daniel J. Bernstein	University of Illinois at Chicago, USA and TU Eindhoven, The Netherlands
Johannes Buchmann	TU Darmstadt, Germany
Claude Crépeau	McGill University, Canada
Jintai Ding	University of Cincinnati, USA
Philippe Gaborit	University of Limoges, France
Tim Güneysu	Ruhr University of Bochum, Germany
Sean Hallgren	Pennsylvania State University, USA
Nadia Heninger	University of Pennsylvania, USA
David Jao	University of Waterloo, Canada
Tanja Lange	TU Eindhoven, The Netherlands

Yi-Kai Liu	NIST, USA
Vadim Lyubashevsky	ENS Paris, France
Michele Mosca	University of Waterloo and Perimeter Institute, Canada
Bart Preneel	KU Leuven, Belgium
Martin Rötteler	Microsoft Research, USA
Nicolas Sendrier	Inria, France
Daniel Smith-Tone	University of Louisville and NIST, USA
Douglas Stebila	QUT, Australia
Damien Stehlé	ENS Lyon, France
Rainer Steinwandt	Florida Atlantic University, USA
Douglas Stinson	University of Waterloo, Canada
Tsuyoshi Takagi	Kyushu University, Japan
Enrico Thomae	operational services GmbH & Co. KG, Germany
Jean-Pierre Tillich	Inria, France
Bo-Yin Yang	Academia Sinica, Taiwan

External Reviewers

Martin Albrecht	Ruud Pellikaan
André Chailloux	Christiane Peters
Julia Chaulet	Albrecht Petzoldt
Jérémie Detrey	Thomas Pöppelmann
Gus Gutoski	Olivier Ruatta
Andreas Hülsing	Peter Schwabe
Stephen Jordan	Fang Song
Zhenhua Liu	Alan Szepieniec
Rafael Misoczki	Frederik Vercauteren
Dustin Moody	Ingo von Maurich
Svetla Nikova	Takanori Yasuda

Partners and Sponsors

CryptoWorks21
Institute for Quantum Computing, University of Waterloo
Microsoft Research
National Science Foundation
Perimeter Institute for Theoretical Physics
The Fields Institute for Research in Mathematical Sciences
Tutte Institute for Mathematics and Computing

Table of Contents