

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

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

Michele Mosca (Ed.)

Post-Quantum Cryptography

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



Springer

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

© Springer International Publishing Switzerland 2014

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, 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.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

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

VIII Organization

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 Chaulot	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

Sealing the Leak on Classical NTRU Signatures	1
<i>Carlos Aguilar Melchor, Xavier Boyen, Jean-Christophe Deneuville, and Philippe Gaborit</i>	
On the Efficiency of Provably Secure NTRU	22
<i>Daniel Cabarcas, Patrick Weiden, and Johannes Buchmann</i>	
A Polynomial-Time Algorithm for Solving a Class of Underdetermined Multivariate Quadratic Equations over Fields of Odd Characteristics . . .	40
<i>Chen-Mou Cheng, Yasufumi Hashimoto, Hiroyuki Miura, and Tsuyoshi Takagi</i>	
Differential Properties of the HFE Cryptosystem	59
<i>Taylor Daniels and Daniel Smith-Tone</i>	
The Cubic Simple Matrix Encryption Scheme	76
<i>Jintai Ding, Albrecht Petzoldt, and Lih-chung Wang</i>	
RankSign: An Efficient Signature Algorithm Based on the Rank Metric	88
<i>Philippe Gaborit, Olivier Ruatta, Julien Schrek, and Gilles Zémor</i>	
Cryptanalysis of the Multivariate Signature Scheme Proposed in PQCrypto 2013	108
<i>Yasufumi Hashimoto</i>	
Attacking Code-Based Cryptosystems with Information Set Decoding Using Special-Purpose Hardware	126
<i>Stefan Heyse, Ralf Zimmermann, and Christof Paar</i>	
Transcript Secure Signatures Based on Modular Lattices	142
<i>Jeff Hoffstein, Jill Pipher, John M. Schanck, Joseph H. Silverman, and William Whyte</i>	
Isogeny-Based Quantum-Resistant Undeniable Signatures	160
<i>David Jao and Vladimir Soukharev</i>	
An Asymptotically Optimal Structural Attack on the ABC Multivariate Encryption Scheme	180
<i>Dustin Moody, Ray Perlner, and Daniel Smith-Tone</i>	

Lattice Cryptography for the Internet	197
<i>Chris Peikert</i>	
Optimizing Information Set Decoding Algorithms to Attack Cyclosymmetric MDPC Codes	220
<i>Ray Perlner</i>	
ZHFE, a New Multivariate Public Key Encryption Scheme	229
<i>Jaiberth Porras, John Baena, and Jintai Ding</i>	
A Note on Quantum Security for Post-Quantum Cryptography	246
<i>Fang Song</i>	
Towards Side-Channel Resistant Implementations of QC-MDPC McEliece Encryption on Constrained Devices	266
<i>Ingo von Maurich and Tim Güneysu</i>	
Author Index	283