Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Zürich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, 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, Saarbrücken, Germany

More information about this series at <http://www.springer.com/series/7410>

Tsuyoshi Takagi (Ed.)

Post-Quantum Cryptography

7th International Workshop, PQCrypto 2016
Fukuoka, Japan, February 24–26, 2016
Proceedings

Springer

Editor
Tsuyoshi Takagi
Kyushu University
Fukuoka
Japan

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-29359-2 ISBN 978-3-319-29360-8 (eBook)
DOI 10.1007/978-3-319-29360-8

Library of Congress Control Number: 2015960429

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing Switzerland 2016

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.

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.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

This Springer imprint is published by SpringerNature
The registered company is Springer International Publishing AG Switzerland

Preface

PQCrypto 2016, the 7th International Workshop on Post-Quantum Cryptography, was held in Fukuoka, Japan, during February 24–26, 2016. It was organized in cooperation with the International Association for Cryptologic Research.

The aim of PQCrypto is to serve as a forum for researchers to present results and exchange ideas on the topic of cryptography in the era of large-scale quantum computers. The workshop was preceded by a winter school during February 22–23, 2016.

PQCrypto 2016 has received 42 submissions from 21 countries all over the world. The Program Committee selected 16 papers for publication in the workshop proceedings. The accepted papers deal with multivariate polynomial cryptography, code-based cryptography, lattice-based cryptography, quantum algorithms, post-quantum protocols, and implementations. The program featured four excellent invited talks given by Daniel Bernstein (University of Illinois at Chicago), Ernie Brickell (Intel), Steven Galbraith (University of Auckland), and Masahide Sasaki (Quantum ICT Laboratory, NICT), as well as a hot topic session. The Program Committee selected the work “An Efficient Attack on a Code-Based Signature Scheme” by Aurélie Phesso and Jean-Pierre Tillich for the Best Paper Award of PQCrypto 2016. During the workshop, the National Institute of Standards and Technology (NIST) announced a preliminary plan for the submission and evaluation of quantum-resistant algorithms for potential standardization.

Many people contributed to the success of PQCrypto 2016. I am very grateful to all of the Program Committee members as well as the external reviewers for their fruitful comments and discussions on their areas of expertise. I am greatly indebted to the general chair, Kouichi Sakurai, for his efforts and overall guidance. I would also like to thank the general co-chairs, Takanori Yasuda and Kirill Morozov, and the local Organizing Committee, Hiroaki Anada, Shinichi Matsumoto, Duong Hoang Dung, Taku Jiromaru, and Emi Watanabe, for their continuous support.

Finally, I would like to express our gratitude to our partners and sponsors: JST CREST, ISIT, ID Quantique, Fukuoka Convention & Visitors Bureau, The Telecommunications Advancement Foundation, and Inoue Foundation for Science. ISIT’s contribution to the organization of this workshop is supported by “Strategic Information and Communications R&D Promotion Programme (SCOPE), no. 0159-0016,” Ministry of Internal Affairs and Communications, Japan.

February 2016

Tsuyoshi Takagi

Organization

General Chair

Kouichi Sakurai Kyushu University and ISIT, Japan

General Co-chairs

Takanori Yasuda ISIT, Japan
Kirill Morozov Kyushu University, Japan

Program Chair

Tsuyoshi Takagi Kyushu University, Japan

Program Committee

Joppe Bos	NXP Semiconductors, Belgium
Johannes Buchmann	TU Darmstadt, Germany
Chen-Mou Cheng	National Taiwan University, Taiwan
Pierre-Louis Cayrel	Jean Monnet University, France
Claude Crépeau	McGill University, Canada
Jintai Ding	University of Cincinnati, USA
Philippe Gaborit	University of Limoges, France
Danilo Gligoroski	Norwegian University of Science and Technology, Norway
Tim Güneysu	Ruhr University of Bochum, Germany
Sean Hallgren	Pennsylvania State University, USA
Yasufumi Hashimoto	University of the Ryukyus, Japan
David Jao	University of Waterloo, Canada
Tanja Lange	TU Eindhoven, The Netherlands
Yi-Kai Liu	NIST, USA
Michele Mosca	University of Waterloo and Perimeter Institute, Canada
Martin Rötteler	Microsoft Research, USA
Nicolas Sendrier	Inria, France
Daniel Smith-Tone	University of Louisville and NIST, USA
Damien Stehlé	ENS Lyon, France
Rainer Steinwandt	Florida Atlantic University, USA
Jean-Pierre Tillich	Inria, France
Keita Xagawa	NTT, Japan
Bo-Yin Yang	Academia Sinica, Taiwan
Zhengfeng Zhang	Chinese Academy of Sciences, China

Local Organizing Committee

Hiroaki Anada	ISIT, Japan
Shinichi Matsumoto	ISIT, Japan
Duong Hoang Dung	Kyushu University, Japan
Taku Jiromaru	Conference Service, Japan
Emi Watanabe	Kyushu University, Japan

External Reviewers

John Baene	Po-Chun Kuo	Fang Song
Shi Bai	Wen-Ding Li	Tobias Schneider
Yun-An Chang	Artur Mariano	Rodolfo Canto Torres
Long Chen	Rafael Misoczki	Saraswathy
Craig Costello	Mohamed Saied	Ramanathapuram
Alain Couvreur	Mohamed	Vancheeswaran
Leo Ducas	Michael Naehrig	Christopher Wolf
Kirsten Eisentraeger	Khoa Nguyen	Jiang Zhang
Vlad Gheorghiu	Edoardo Persichetti	
Gerhard Hoffman	Simona Samardjiska	

Steering Committee

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
Tanja Lange	TU 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

Partners and Sponsors

CREST, Japan Science and Technology Agency
 Institute of Systems, Information Technologies and Nanotechnologies (ISIT)
 ID Quantique
 Fukuoka Convention and Visitors Bureau
 The Telecommunications Advancement Foundation
 Inoue Foundation for Science

Contents

IND-CCA Secure Hybrid Encryption from QC-MDPC Niederreiter	1
<i>Ingo von Maurich, Lukas Heberle, and Tim Güneysu</i>	
RankSynd a PRNG Based on Rank Metric	18
<i>Philippe Gaborit, Adrien Hauteville, and Jean-Pierre Tillich</i>	
Applying Grover’s Algorithm to AES: Quantum Resource Estimates	29
<i>Markus Grassl, Brandon Langenberg, Martin Roetteler, and Rainer Steinwandt</i>	
Post-Quantum Security of the CBC, CFB, OFB, CTR, and XTS Modes of Operation	44
<i>Mayuresh Vivekanand Anand, Ehsan Ebrahimi Targhi, Gelo Noel Tabia, and Dominique Unruh</i>	
Post-Quantum Security Models for Authenticated Encryption	64
<i>Vladimir Soukharev, David Jao, and Srinath Seshadri</i>	
Quantum Collision-Resistance of Non-uniformly Distributed Functions	79
<i>Ehsan Ebrahimi Targhi, Gelo Noel Tabia, and Dominique Unruh</i>	
An Efficient Attack on a Code-Based Signature Scheme	86
<i>Aurélie Phesso and Jean-Pierre Tillich</i>	
Vulnerabilities of “McEliece in the World of Escher”	104
<i>Dustin Moody and Ray Perlner</i>	
Cryptanalysis of the McEliece Public Key Cryptosystem Based on Polar Codes	118
<i>Magali Bardet, Julia Chaulet, Vlad Dragoi, Ayoub Otmani, and Jean-Pierre Tillich</i>	
Analysis of Information Set Decoding for a Sub-linear Error Weight	144
<i>Rodolfo Canto Torres and Nicolas Sendrier</i>	
On the Differential Security of the HFEv- Signature Primitive	162
<i>Ryann Cartor, Ryan Gipson, Daniel Smith-Tone, and Jeremy Vates</i>	
Extension Field Cancellation: A New Central Trapdoor for Multivariate Quadratic Systems	182
<i>Alan Szepieniec, Jintai Ding, and Bart Preneel</i>	
Security Analysis and Key Modification for ZHFE	197
<i>Ray Perlner and Daniel Smith-Tone</i>	

Efficient ZHFE Key Generation	213
<i>John B. Baena, Daniel Cabarcas, Daniel E. Escudero,</i> <i>Jaiberth Porras-Barrera, and Javier A. Verbel</i>	
Additively Homomorphic Ring-LWE Masking	233
<i>Oscar Reparaz, Ruan de Clercq, Sujoy Sinha Roy, Frederik Vercauteren,</i> <i>and Ingrid Verbauwhede</i>	
A Homomorphic LWE Based E-voting Scheme	245
<i>Ilaria Chillotti, Nicolas Gama, Mariya Georgieva,</i> <i>and Malika Izabachène</i>	
Author Index	267