Lecture Notes in Computer Science 7932

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

Philippe Gaborit (Ed.)

Post-Quantum Cryptography

5th International Workshop, PQCrypto 2013
Limoges, France, June 4-7, 2013
Proceedings

Volume Editor

Philippe Gaborit
University of Limoges
XLIM Laboratory, Department DMI
123, Avenue Albert Thomas, 87000 Limoges, France
E-mail: gaborit@unilim.fr

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-38615-2 e-ISBN 978-3-642-38616-9
DOI 10.1007/978-3-642-38616-9
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2013938951

CR Subject Classification (1998): E.3, K.6.5, D.4.6, F.2, G.2.1, E.4, C.2.0

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 2013, the 5th International Workshop on Post-Quantum Cryptography was held in Limoges, France, during June 4–7, 2013.

The workshop attracted 24 submissions, of which the Program Commmittee selected 17 for publication in the workshop proceedings. The accepted papers dealt with the topics of code-based cryptography, lattice-based cryptography, multivariate-cryptography, and cryptanalysis or implementations. The Program Committee included 23 subject-matter experts from 11 countries.

The workshop included two invited talks by Frédéric Magniez and Michael Naehrig and a recent results session chaired by Carlos Aguilar Melchor.

I would like to thank all the Program Committee members, who made great effort contributing their time, knowledge, and expertise. I also thank the external reviewers who assisted in the process.

I wish to thank the generous sponsors of PQCRypto 2013: the Region Limousin, the Limoges University, the Mathematics and Computer Science Departement of the XLIM laboratory and the XLIM laboratory. Special thanks are also due to Thierry Berger for his organizational effort as General Chair and to Odile Duval and Jean-Christophe Deneuville for their everyday help.

April 2013 Philippe Gaborit

Organization

General Chair

Thierry Berger	Limoges University, France

Program Chair

Philippe Gaborit	Limoges University, France

Steering Committee

Daniel J. 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	University of Limoges, France
Tanja Lange	Technische Universiteit Eindhoven, The Netherlands
Daniele Micciancio	University of California, San Diego, USA
Werner Schindler	BSI, Germany
Nicolas Sendrier	INRIA, France
Shigeo Tsujii	Chuo University, Japan
Bo-Yin Yang	Academia Sinica, Taiwan

Program Committee

Carlos Aguilar Melchor	University of Limoges, France
Paulo Barreto	University of Sao Paulo, Brazil
Daniel J. Bernstein	University of Illinois at Chicago, USA
Xavier Boyen	QUT, Australia
Johannes Buchmann	TU Darmstadt, Germany
Stanislav Bulygin	TU Darmstadt, Germany
Claude Crépeau	McGill University, Canada
Jintai Ding	University of Cincinnati, USA
Pierre-Alain Fouque	University of Rennes I, France
Tim Guneysu	Rhur University Bochum, Germany
Sean Hallgren	University of Pennsylvania, USA
Kazukuni Kobara	AIST, Japan
Tanja Lange	TU Eindhoven, The Netherlands
Gregor Leander	Danmarks TU, Denmark

Michele Mosca	University of Waterloo, Canada
Bart Preneel	KU Leuven, Belgium
Michael Schneider	TU Darmstadt, Germany
Nicolas Sendrier	INRIA, France
Damien Stehlé	ENS Lyon, France
Jean-Pierre Tillich	INRIA, France
Bo-Yin Yang	Academia Sinica, Taiwan

External Reviewers

François Arnault
Rafael Baiao
Daniel Cabarcas
Jie Chen
Ming-Shing Chen
Adama Diene
Vivien Dubois
Nicolas Gama
Valérie Gauthier Umaña
Stefan Heyse
Jeffrey Hoffstein
Lei Hu
Andreas Hülsing
Rafael Misoczki
Kirill Morozov
Khoa Nguyen (special thanks)
Ryo Nojima
Ayoub Otmani
Christiane Peters
Albrecht Petzold
Thomas Pöppelmann
Koichi Sakumoto
John Schanck
Dimitris E. Simos
Yasuda Takanori
Chendong Tao
Enrico Thomae (special thanks)
Joop van de Pol
Ingo von Maurich
Patrick Weiden
Christopher Wolf
C.-H. Yu

Table of Contents