

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

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

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

Philippe Gaborit (Ed.)

Post-Quantum Cryptography

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



Springer

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

© Springer-Verlag Berlin Heidelberg 2013

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

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

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 Committee 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 Department 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

VIII Organization

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

Table of Contents

Using LDGM Codes and Sparse Syndromes to Achieve Digital Signatures	1
<i>Marco Baldi, Marco Bianchi, Franco Chiaraluce, Joachim Rosenthal, and Davide Schipani</i>	
Quantum Algorithms for the Subset-Sum Problem	16
<i>Daniel J. Bernstein, Stacey Jeffery, Tanja Lange, and Alexander Meurer</i>	
Improved Lattice-Based Threshold Ring Signature Scheme	34
<i>Slim Bettaieb and Julien Schrek</i>	
Degree of Regularity for HFEv and HFEv-	52
<i>Jintai Ding and Bo-Yin Yang</i>	
Software Speed Records for Lattice-Based Signatures	67
<i>Tim Güneysu, Tobias Oder, Thomas Pöppelmann, and Peter Schwabe</i>	
Solving the Shortest Vector Problem in Lattices Faster Using Quantum Search	83
<i>Thijs Laarhoven, Michele Mosca, and Joop van de Pol</i>	
An Efficient Attack of a McEliece Cryptosystem Variant Based on Convolutional Codes	102
<i>Grégory Landais and Jean-Pierre Tillich</i>	
Extended Algorithm for Solving Underdefined Multivariate Quadratic Equations	118
<i>Hiroyuki Miura, Yasufumi Hashimoto, and Tsuyoshi Takagi</i>	
Quantum Key Distribution in the Classical Authenticated Key Exchange Framework	136
<i>Michele Mosca, Douglas Stebila, and Berkant Ustaoglu</i>	
Cryptanalysis of Hash-Based Tamed Transformation and Minus Signature Scheme	155
<i>Xuyun Nie, Zhaohu Xu, and Johannes Buchmann</i>	
A Classification of Differential Invariants for Multivariate Post-quantum Cryptosystems	165
<i>Ray Perlner and Daniel Smith-Tone</i>	

Secure and Anonymous Hybrid Encryption from Coding Theory	174
<i>Edoardo Persichetti</i>	
Fast Verification for Improved Versions of the UOV and Rainbow Signature Schemes	188
<i>Albrecht Petzoldt, Stanislav Bulygin, and Johannes Buchmann</i>	
The Hardness of Code Equivalence over \mathbb{F}_q and Its Application to Code-Based Cryptography	203
<i>Nicolas Sendrier and Dimitris E. Simos</i>	
Timing Attacks against the Syndrome Inversion in Code-Based Cryptosystems	217
<i>Falko Strenzke</i>	
Simple Matrix Scheme for Encryption	231
<i>Chengdong Tao, Adama Diene, Shaohua Tang, and Jintai Ding</i>	
Multivariate Signature Scheme Using Quadratic Forms	243
<i>Takanori Yasuda, Tsuyoshi Takagi, and Kouichi Sakurai</i>	
Author Index	259