Lecture Notes in Computer Science 5299

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

Johannes Buchmann Jintai Ding (Eds.)

Post-Quantum Cryptography

Second International Workshop, PQCrypto 2008
Cincinnati, OH, USA, October 17-19, 2008
Proceedings

Springer

Volume Editors

Johannes Buchmann
Technische Universität Darmstadt
Fachbereich Informatik
Hochschulstraße 10, 64289 Darmstadt, Germany
E-mail: buchmann@cdc.informatik.tu-darmstadt.de

Jintai Ding
The University of Cincinnati
Department of Mathematical Sciences
P.O. Box 210025, Cincinnati, OH 45221-0025, USA
E-mail: jintai.ding@uc.edu

Library of Congress Control Number: 2008936091

CR Subject Classification (1998): E.3, D.4.6, K.6.5, F.2.1-2, C.2, H.4.3

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-88402-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-88402-6 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12538829 06/3180 5 4 3 2 1 0

Preface

Three decades ago public-key cryptosystems made a revolutionary breakthrough in cryptography. They have developed into an indispensable part of our modern communication system. In practical applications RSA, DSA, ECDSA, and similar public key cryptosystems are commonly used. Their security depends on assumptions about the difficulty of certain problems in number theory, such as the Integer Prime Factorization Problem or the Discrete Logarithm Problem.

However, in 1994 Peter Shor showed that quantum computers could break any public-key cryptosystem based on these hard number theory problems. This means that if a reasonably powerful quantum computer could be built, it would put essentially all modern communication into peril. In 2001, Isaac Chuang and Neil Gershenfeld implemented Shor's algorithm on a 7-qubit quantum computer. In 2007 a 16-qubit quantum computer was demonstrated by a start-up company with the prediction that a 512-qubit or even a 1024-qubit quantum computer would become available in 2008. Some physicists predicted that within the next 10 to 20 years quantum computers will be built that are sufficiently powerful to implement Shor's ideas and to break all existing public key schemes. Thus we need to look ahead to a future of quantum computers, and we need to prepare the cryptographic world for that future.

The research community has put much effort into developing quantum computers and at the same time searching for alternative public-key cryptosystems that could resist these quantum computers. Post-quantum cryptography is a new fast developing area, where public key cryptosystems are studied that could resist these emerging attacks. Currently there are four families of public-key cryptosystems that have the potential to resist quantum computers: the code-based public-key cryptosystems, the hash-based public-key cryptosystems, the lattice-based public-key cryptosystems and the multivariate public-key cryptosystems.

Clearly there is a need to organize an event for researchers working in this area to present their results, to exchange ideas and, most importantly, to allow the world to know what is the state of art of research in this area. In May of 2006, the First International Workshop on Post-Quantum Cryptography was held at the Catholic University of Louven in Belgium with support from the European Network of Excellence for Cryptology (ECRYPT), funded within the Information Societies Technology Programme (IST) of the European Commission's Sixth Framework Programme. This workshop did not have formal proceedings.

PQCrypto 2008, the Second International Workshop on Post-Quantum Cryptography, was held at the University of Cincinnati in Cincinnati, USA, October 17–19. This meeting was sponsored by the University of Cincinnati, the Taft Research Center and FlexSecure®GmbH. This workshop had a devoted international Program Committee, who worked very hard to evaluate and select the high-quality papers for presentations. Each paper was anonymously reviewed by

at least three Program Committee members. Revised versions of the accepted papers are published in these proceedings.

We would like to thank all the authors for their support in submitting their papers and the authors of the accepted papers for their efforts in making these proceedings possible on time. We are very grateful to the Program Committee members for devoting for their time and efforts in reviewing and selecting the papers and we are also very grateful to the external reviewers for their efforts.

We would like to thank the efforts of the local Organization Committee, in particular, Timothy Hodges and Dieter Schmidt, without whose support this workshop would not be possible. We would also like to thank Richard Harknett, Chair of the Taft research center, for his support.

We would like to thank the Easychair electronic conference system, which made the handling of the submission and reviewing process easy and efficient. In addition, we would like to thank Daniel Cabarcas for managing all the electronic processes.

We would also like to thank Springer, in particular Alfred Hofmann and Anna Kramer for their support in publishing these proceedings.

August 2008

Johannes Buchmann
Jintai Ding

Organization

PQCrypto 2008 was organized by the Department of Mathematical Sciences, University of Cincinnati.

Executive Committee

Program Chairs	Johannes Buchmann (Technical University of Darmstadt)
	Jintai Ding (University of Cincinnati)
General Chair	Timothy Hodges (University of Cincinnati)
Local Committee	Timothy Hodges (University of Cincinnati)
	Jintai Ding (University of Cincinnati)
	Dieter Schmidt (University of Cincinnati)

Program Committee

Gernot Albert, Germany
Koichiro Akiyama, Japan
Daniel J. Bernstein, USA
Claude Crepeau, Canada
Cunshen Ding, China
Bao Feng, Singapore
Louis Goubin, France
Tor Helleseth, Norway
Tanja Lange, The Netherlands
Christof Paar, Germany
Louis Salvail, Denmark
Werner Schindler, Germany
Nicolas Sendrier, France
Alice Silverberg, USA
Martijn Stam, Switzerland
Michael Szydlo, USA
Shigeo Tsujii, Japan
Thomas Walther, Germany
Chaoping Xing, Singapore
Bo-yin Yang, Taipei

Referees

G. Albert
K. Akiyama
R. Avanzi
J. Baena
D. Bernstein
J. Buchmann
D. Cabarcas
C. Clough
C. Crepeau
A. Diene
C. Ding
J. Ding
B. Feng
R. Fujita
P. Gaborit
M. Gotaishi
L. Goubin
T. Helleseth
T. Lange
X. Nie
C. Paar
L. Salvail
W. Schindler
N. Sendrier
A. Silverberg
M. Stam
M. Szydlo
K. Tanaka
S. Tsujii
T. Walther
C. Xing
B. Yang

Sponsors

The Taft Research Center at the University of Cincinnati
Department of Mathematical Sciences, University of Cincinnati
FlexSecure®GmbH, Darmstadt, Germany

Table of Contents