Bo-Yin Yang (Ed.)

Post-Quantum Cryptography

4th International Workshop, PQCrypto 2011
Taipei, Taiwan, November 29 – December 2, 2011
Proceedings

Springer
Foreword


A decade had passed and large quantum computers did not actually appear, but it seemed clear enough that the cryptographic research community should not await ostrich-like for the first public appearance of quantum computing to look for alternatives to RSA.

It was in this atmosphere that we saw the emergence, and in some cases renaissance, of “alternative” approaches to public-key cryptography that would survive quantum computers, for which the term “post-quantum cryptography” was affectionately coined.

Cryptographers were hard at work looking for new possibilities for public-key cryptosystems that could resist quantum computers, and currently there are four major families of post-quantum public-key cryptosystems: the code-based public-key cryptosystems, the hash-based public-key cryptosystems, the lattice-based public-key cryptosystems and the multivariate public-key cryptosystems. Many possibilities were proposed and quite a few were rejected. With the increase of research activity in post-quantum cryptography, it became clear that a venue is needed where ideas can be exchanged, results can be presented, and the newest developments can be made known to the world.

Thus was born the first Post-Quantum Cryptography, or PQCrypto, workshop in May 2006 in Leuven. This workshop did not have formal proceedings, and was only made possible with support of the European Union’s Framework Program project ECRYPT. PQCrypto 2006 was such a success, however, that Post-Quantum Cryptography was encouraged to form a Steering Committee and run two more instances of these workshop in 2008 (October in Cincinnati, USA) and 2010 (May in Darmstadt, Germany).

The fourth event of this series, PQCrypto 2011, was organized in Taipei, Taiwan, by the Department of Electrical Engineering at the National Taiwan University during November 29–December 2, 2011. The Program Committee received 38 proposals of contributed talks from which 18 were selected. Each paper was thoroughly examined by several independent experts from the Program Committee and additional external reviewers. The papers along with the reviews were then scrutinized by the Program Committee members during a discussion phase after which recommendations were given to all authors. In several
cases, we required the authors to work with a shepherd to ensure that the text was edited in accordance with the committee comments and a high standard of writing. Revised versions of the accepted contributions are published in these proceedings.

Thanks must go to all authors for submitting their quality research work to the conference. Even more deserving are the Program Committee and our external reviewers for their time and energy to ensure that a conference program and a volume of high scientific quality could be assembled.

I thank my fellow organizers: Chen-Mou Cheng, who made all the worldly arrangements, and Peter Schwabe, our capable indefatigable webmaster. We would also like to thank Springer, in particular Alfred Hofmann and Anna Kramer, for their support in publishing these proceedings.

September 2011

Bo-Yin Yang
### Organization

PQCrypto 2011 was organized by the Department of Electrical Engineering at the National Taiwan University, Taipei, Taiwan; we thank Intel, the National Science Council of Taiwan, and Academia Sinica for sponsorship.

### General Chair

Chen-Mou (Doug) Cheng  
National Taiwan University, Taiwan

### Program Chair

Bo-Yin Yang  
Academia Sinica, Taiwan

### Program Committee

<table>
<thead>
<tr>
<th>Name</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Martin R. Albrecht</td>
<td>Université Pierre et Marie Curie, France</td>
</tr>
<tr>
<td>Paulo S.L.M. Barreto</td>
<td>Universidade de São Paulo, Brazil</td>
</tr>
<tr>
<td>Daniel J. Bernstein</td>
<td>University of Illinois at Chicago, USA</td>
</tr>
<tr>
<td>Johannes A. Buchmann</td>
<td>Technische Universität Darmstadt, Germany</td>
</tr>
<tr>
<td>Jintai Ding</td>
<td>University of Cincinnati, USA</td>
</tr>
<tr>
<td>Vivien Dubois</td>
<td>Direction générale de l’armement, France</td>
</tr>
<tr>
<td>Louis Goubin</td>
<td>Université de Versailles, France</td>
</tr>
<tr>
<td>Sean Hallgren</td>
<td>Pennsylvania State University, USA</td>
</tr>
<tr>
<td>Lars Knudsen</td>
<td>Danmarks Tekniske Universitet, Denmark</td>
</tr>
<tr>
<td>Tanja Lange</td>
<td>Technische Universiteit Eindhoven, The Netherlands</td>
</tr>
<tr>
<td>Richard Lindner</td>
<td>Technische Universität Darmstadt, Germany</td>
</tr>
<tr>
<td>Vadim Lyubashevsky</td>
<td>École Normale Supérieure Paris, France</td>
</tr>
<tr>
<td>Daniele Micciancio</td>
<td>University of California at San Diego, USA</td>
</tr>
<tr>
<td>Michele Mosca</td>
<td>University of Waterloo, Canada</td>
</tr>
<tr>
<td>Chris Peikert</td>
<td>Georgia Institute of Technology, USA</td>
</tr>
<tr>
<td>Christiane Peters</td>
<td>Technische Universiteit Eindhoven, The Netherlands</td>
</tr>
<tr>
<td>Bart Preneel</td>
<td>Katholieke Universiteit Leuven, Belgium</td>
</tr>
<tr>
<td>Nicolas Sendrier</td>
<td>INRIA Paris-Rocquencourt, France</td>
</tr>
<tr>
<td>Damien Stehlé</td>
<td>CNRS and École Normale Supérieure de Lyon, France</td>
</tr>
<tr>
<td>Jean-Pierre Tillich</td>
<td>INRIA Paris-Rocquencourt, France</td>
</tr>
<tr>
<td>Ralf-Philipp Weinmann</td>
<td>Université du Luxembourg, Luxembourg</td>
</tr>
<tr>
<td>Christopher Wolf</td>
<td>Ruhr-Universität Bochum, Germany</td>
</tr>
</tbody>
</table>
Webmaster

Peter Schwabe National Taiwan University, Taiwan

External Reviewers

Romain Alleaume  Gerhard Hoffmann  Louis Salvail
Thierry Berger  Jeff Hoffstein  Michael Schneider
Gaëtan Bisson  Andreas Hülsing  Julien Schrek
Stanislav Bulygin  Po-Chun Kuo  Jieh-Ren Jarron Shih
Jean-Marc Couveignes  Feng-Hao Liu  Boris Skoric
Christina Delfs  Pierre Loidreau  Benjamin Smith
Kirsten Eisenträger  Alexander Meurer  Douglas Stebila
Pooya Farshim  Rafael Misoczki  Andreas Stein
Thomas Feller  Petros Mol  Ron Steinfeld
Matthieu Finiasz  Michael Naehrig  Enrico Thomae
Philippe Gaborit  Robert Niebuhr  Valerie Gauthier Umana
Steven Galbraith  Jacques Patarin  Frederik Vercauteren
Nicolas Gama  Kenny Paterson  William Whyte
Ryan Henry  Ludovic Perret
Jens Hermans  Edoardo Persichetti
Stefan Heyse  Albrecht Petzoldt

PQCrypto Steering Committee

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

Sponsoring Institutions

Institute of Information Science, Academia Sinica
Center of Information Technology and Innovation, Academia Sinica
The Intel Connected Context Computing Center (at National Taiwan University)
# Table of Contents

General Fault Attacks on Multivariate Public Key Cryptosystems .... 1  
*Yasufumi Hashimoto, Tsuyoshi Takagi, and Kouichi Sakurai*

Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies .......................... 19  
*David Jao and Luca De Feo*

Full Cryptanalysis of the Chen Identification Protocol .............. 35  
*Philippe Gaborit, Julien Schrek, and Gilles Zémor*

Decoding One Out of Many ..................................... 51  
*Nicolas Sendrier*

On Provable Security of UOV and HFE Signature Schemes against Chosen-Message Attack .................................. 68  
*Koichi Sakumoto, Taizo Shirai, and Harunaga Hiwatari*

Roots of Square: Cryptanalysis of Double-Layer Square and Square+ ... 83  
*Enrico Thomae and Christopher Wolf*

An Efficient Attack on All Concrete KKS Proposals .................. 98  
*Ayoub Otmani and Jean-Pierre Tillich*

XMSS – A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions .......................... 117  
*Johannes Buchmann, Erik Dahmen, and Andreas Hülsing*

On the Differential Security of Multivariate Public Key Cryptosystems ........................................ 130  
*Daniel Smith-Tone*

Implementation of McEliece Based on Quasi-dyadic Goppa Codes for Embedded Devices .......................... 143  
*Stefan Heyse*

Efficient Threshold Encryption from Lossy Trapdoor Functions ........ 163  
*Xiang Xie, Rui Xue, and Rui Zhang*

Monoidic Codes in Cryptography .................................. 179  
*Paulo S.L.M. Barreto, Richard Lindner, and Rafael Misoczki*

Simplified High-Speed High-Distance List Decoding for Alternant Codes ........................................ 200  
*Daniel J. Bernstein*
Statistical Decoding of Codes over $\mathbb{F}_q$ .......................... 217

Robert Niebuhr

High-Speed Hardware Implementation of Rainbow Signature on FPGAs .......................................................... 228

Shaohua Tang, Haibo Yi, Jintai Ding, Huan Chen, and Guomin Chen

Wild McEliece Incognito ............................................ 244

Daniel J. Bernstein, Tanja Lange, and Christiane Peters

A New Spin on Quantum Cryptography: Avoiding Trapdoors and Embracing Public Keys ................................. 255

Lawrence M. Ioannou and Michele Mosca


Takanori Yasuda and Kouichi Sakurai

Author Index .......................................................... 295