# Lecture Notes in Computer Science 6487

Marc Joye Atsuko Miyaji Akira Otsuka (Eds.)

# Pairing-Based Cryptography – Pairing 2010

4th International Conference
Yamanaka Hot Spring, Japan, December 13-15, 2010
Proceedings

Springer

Volume Editors

Marc Joye
Technicolor, Security and Content Protection Labs
35576 Cesson-Sévigné Cedex, France
E-mail: marc.joye@technicolor.com

Atsuko Miyaji
Japan Advanced Institute of Science and Technology (JAIST)
Nomi, Ishikawa 923-1292, Japan
E-mail: miyaji@jaist.ac.jp

Akira Otsuka
National Institute of Advanced Industrial Science and Technoloy (AIST)
Tokyo 101-0021, Japan
E-mail: a-otsuka@aist.go.jp

Library of Congress Control Number: 2010939850

CR Subject Classification (1998): E.3, K.6.5, D.4.6, C.2, E.4, I.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-17454-X Springer Berlin Heidelberg New York
ISBN-13 978-3-642-17454-4 Springer Berlin Heidelberg New York

springer.com

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

# Preface

The 4th International Conference on Pairing-Based Cryptography (Pairing 2010) was held in Yamanaka Hot Spring, Japan, during December 13-15, 2010. It was jointly co-organized by the National Institute of Advanced Industrial Science and Technology (AIST), Japan, and the Japan Advanced Institute of Science and Technology (JAIST).

The goal of Pairing 2010 was to bring together leading researchers and practitioners from academia and industry, all concerned with problems related to pairing-based cryptography. We hope that this conference enhanced communication among specialists from various research areas and promoted creative interdisciplinary collaboration.

The conference received 64 submissions from 17 countries, out of which 25 papers from 13 countries were accepted for publication in these proceedings. At least three Program Committee (PC) members reviewed each submitted paper, while submissions co-authored by a PC member were submitted to the more stringent evaluation of five PC members. In addition to the PC members, many external reviewers joined the review process in their particular areas of expertise. We were fortunate to have this energetic team of experts, and are deeply grateful to all of them for their hard work, which included a very active discussion phase. The paper submission, review and discussion processes were effectively and efficiently made possible by the Web-based system iChair.

Furthermore, the conference featured three invited speakers: Jens Groth from University College London, Joseph H. Silverman from Brown University, and Gene Tsudik from University of California at Irvine, whose lectures on cutting-edge research areas— "Pairing-Based Non-interactive Zero-Knowledge Proofs," "A Survey of Local and Global Pairings on Elliptic Curves and Abelian Varieties," and "Some Security Topics with Possible Applications for Pairing-Based Cryptography," respectively— contributed in a significant part to the richness of the program.

We are very grateful to our supporters and sponsors. In addition to AIST and JAIST, the event was supported by the Special Interest Group on Computer Security (CSEC), IPSJ, Japan, the Japan Technical Group on Information Security (ISEC), IEICE, Japan, and the Technical Committee on Information and Communication System Security (ICSS), IEICE, Japan, and co-sponsored by the National Institute of Information and Communications Technology (NICT), Japan, Microsoft Research, Voltage Security, Hitachi, Ltd., and NTT Data.

Finally, we thank all the authors who submitted papers to this conference, the Organizing Committee members, colleagues and student helpers for their valuable time and effort, and all the conference attendees who made this event a truly intellectually stimulating one through their active participation.

December 2010

Marc Joye
Atsuko Miyaji
Akira Otsuka

# Pairing 2010
# The 4th International Conference on Pairing-Based Cryptography

*Jointly organized by*

National Institute of Advanced Industrial Science and Technology (AIST)
*and*
Japan Advanced Institute of Science and Technology (JAIST)

## General Chair

| | |
|---|---|
| Akira Otsuka | AIST, Japan |

## Program Co-chairs

| | |
|---|---|
| Marc Joye | Technicolor, France |
| Atsuko Miyaji | JAIST, Japan |

## Organizing Committee

| | |
|---|---|
| Local Arrangements Co-chairs | Shoichi Hirose (University of Fukui, Japan)<br>Natsume Matsuzaki (Panasonic, Japan)<br>Kazumasa Omote (JAIST, Japan)<br>Yuji Suga (IIJ, Japan)<br>Tsuyoshi Takagi (Kyushu University, Japan) |
| Finance Co-chairs | Mitsuhiro Hattori (Mitsubishi Electric, Japan)<br>Shoko Yonezawa (AIST, Japan) |
| Publicity Co-chairs | Tomoyuki Asano (Sony, Japan)<br>Tetsutaro Kobayashi (NTT Labs, Japan)<br>Ryo Nojima (NICT, Japan) |
| Liaison Co-chairs | Hiroshi Doi (IISEC, Japan)<br>Masaki Inamura (KDDI R&D Labs Inc., Japan)<br>Toshihiko Matsuo (NTT Data, Japan) |
| System Co-chairs | Nuttapong Attrapadung (AIST, Japan)<br>Atsuo Inomata (NAIST, Japan)<br>Yasuharu Katsuno (IBM Research - Tokyo, Japan)<br>Dai Yamamoto (Fujitsu Laboratories, Japan)<br>Toshihiro Yamauchi (Okayama University, Japan) |
| Publication Co-chairs | Goichiro Hanaoka (AIST, Japan)<br>Takeshi Okamoto (Tsukuba University of Technology, Japan) |

| | |
|---|---|
| Registration Co-chairs | Hideyuki Miyake (Toshiba, Japan)<br>Katsuyuki Okeya (Hitachi, Japan) |

## Program Committee

| | |
|---|---|
| Michel Abdalla | Ecole Normale Supérieure and CNRS, France |
| Paulo S.L.M. Barreto | University of São Paulo, Brazil |
| Daniel Bernstein | University of Illinois at Chicago, USA |
| Jean-Luc Beuchat | University of Tsukuba, Japan |
| Xavier Boyen | Université de Liège, Belgium |
| Ee-Chien Chang | National University of Singapore, Singapore |
| Liqun Chen | HP Labs, UK |
| Reza Rezaeian Farashahi | Macquarie University, Australia |
| David Mandell Freeman | Stanford University, USA |
| Jun Furukawa | NEC Corporation, Japan |
| Craig Gentry | IBM Research, USA |
| Juan González Nieto | Queensland University of Technology, Australia |
| Vipul Goyal | Microsoft Research, India |
| Shai Halevi | IBM Research, USA |
| Antoine Joux | University of Versailles and DGA, France |
| Jonathan Katz | University of Maryland, USA |
| Kwangjo Kim | KAIST, Korea |
| Kristin Lauter | Microsoft Research, USA |
| Pil Joong Lee | Pohang University of Science and Technology, Korea |
| Reynald Lercier | DGA and Université de Rennes, France |
| Benoît Libert | Université Catholique de Louvain, Belgium |
| Mark Manulis | TU Darmstadt, Germany |
| Giuseppe Persiano | Università di Salerno, Italy |
| C. Pandu Rangan | IIT Madras, India |
| Christophe Ritzenthaler | IML, France |
| Germán Sáez | UPC, Spain |
| Michael Scott | Dublin City University, Ireland |
| Alice Silverberg | University of California at Irvine, USA |
| Katsuyuki Takashima | Mitsubishi Electric, Japan |
| Keisuke Tanaka | Tokyo Institute of Technology, Japan |
| Edlyn Teske | University of Waterloo, Canada |
| Frederik Vercauteren | K.U. Leuven, Belgium |
| Bogdan Warinschi | University of Bristol, UK |
| Duncan S. Wong | City University of Hong Kong, China |
| Bo-Yin Yang | Academia Sinica, Taiwan |
| Sung-Ming Yen | National Central University, Taiwan |
| Fangguo Zhang | Sun Yat-sen University, P.R. China |
| Jianying Zhou | I2R, Singapore |

## External Reviewers

Joonsang Baek, Angelo De Caro, Wouter Castryck, Emanuele Cesena, Melissa Chase, Kuo-Zhe Chiou, Sherman Chow, Cheng-Kang Chu, Iwen Coisel, Vanesa Daza, Jérémie Detrey, Sungwook Eom, Essam Ghadafi, Goichiro Hanaoka, Javier Herranz, Qiong Huang, Xinyi Huang, Vincenzo Iovino, David Jao, Ezekiel Kachisa, Dalia Khader, Woo Chun Kim, Fabien Laguillaumie, Tanja Lange, Wei-Chih Lien, Hsi-Chung Lin, Georg Lippold, Jerome Milan, Michael Naehrig, Toru Nakanishi, Greg Neven, Daniel Page, Elizabeth Quaglia, Carla Rafols, Francisco Rodríguez-Henríquez, Alexandre Ruiz, Peter Schwabe, Sharmila Deva Selvi, Jae Woo Seo, Hakan Seyalioglu, Andrew Shallue, Igor Shparlinski, Dan Shumow, Kate Stange, Dongdong Sun, Koutarou Suzuki, Jheng-Hong Tu, Sree Vivek, Christian Wachsmann, Jia Xu, Lingling Xu, Greg Zaverucha, Ye Zhang, Xing-wen Zhao

# Table of Contents

## Efficient Software Implementation

## Invited Talk 1

## Digital Signatures

## Cryptographic Protocols

## Key Agreement

## Invited Talk 2

## Applications: Code Generation, Time-Released Encryption, Cloud Computing

## Point Encoding and Pairing-Friendly Curves

## ID-Based Encryption Schemes

## Invited Talk 3

## Efficient Hardware, FPGAs, and Algorithms