

*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*

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 Technology (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

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.

springer.com

© Springer-Verlag Berlin Heidelberg 2010  
Printed in Germany

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

Registration Co-chairs	Hideyuki Miyake (Toshiba, Japan) 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, Xingwen Zhao



# Table of Contents

## Efficient Software Implementation

An Analysis of Affine Coordinates for Pairing Computation . . . . .	1
<i>Kristin Lauter, Peter L. Montgomery, and Michael Naehrig</i>	
High-Speed Software Implementation of the Optimal Ate Pairing over Barreto–Naehrig Curves . . . . .	21
<i>Jean-Luc Beuchat, Jorge E. González-Díaz, Shigeo Mitsunari, Eiji Okamoto, Francisco Rodríguez-Henríquez, and Tadanori Teruya</i>	

## Invited Talk 1

Some Security Topics with Possible Applications for Pairing-Based Cryptography (Abstract) . . . . .	40
<i>Gene Tsudik</i>	

## Digital Signatures

A New Construction of Designated Confirmer Signature and Its Application to Optimistic Fair Exchange . . . . .	41
<i>Qiong Huang, Duncan S. Wong, and Willy Susilo</i>	
Anonymizable Signature and Its Construction from Pairings . . . . .	62
<i>Fumitaka Hoshino, Tetsutaro Kobayashi, and Koutarou Suzuki</i>	
Identification of Multiple Invalid Pairing-Based Signatures in Constrained Batches . . . . .	78
<i>Brian J. Matt</i>	

## Cryptographic Protocols

Oblivious Transfer with Access Control: Realizing Disjunction without Duplication . . . . .	96
<i>Ye Zhang, Man Ho Au, Duncan S. Wong, Qiong Huang, Nikos Mamoulis, David W. Cheung, and Siu-Ming Yiu</i>	
Increased Resilience in Threshold Cryptography: Sharing a Secret with Devices That Cannot Store Shares . . . . .	116
<i>Koen Simoens, Roel Peeters, and Bart Preneel</i>	
Shorter Verifier-Local Revocation Group Signature with Backward Unlinkability . . . . .	136
<i>Lingbo Wei and Jianwei Liu</i>	

## Key Agreement

Strongly Secure Two-Pass Attribute-Based Authenticated Key Exchange .....	147
<i>Kazuki Yoneyama</i>	
Constructing Certificateless Encryption and ID-Based Encryption from ID-Based Key Agreement .....	167
<i>Dario Fiore, Rosario Gennaro, and Nigel P. Smart</i>	
Ephemeral Key Leakage Resilient and Efficient ID-AKEs That Can Share Identities, Private and Master Keys .....	187
<i>Atsushi Fujioka, Koutarou Suzuki, and Berkant Ustaoglu</i>	

## Invited Talk 2

Pairing-Based Non-interactive Zero-Knowledge Proofs (Abstract) .....	206
<i>Jens Groth</i>	

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

Designing a Code Generator for Pairing Based Cryptographic Functions .....	207
<i>Luis J. Dominguez Perez and Michael Scott</i>	
Efficient Generic Constructions of Timed-Release Encryption with Pre-open Capability .....	225
<i>Takahiro Matsuda, Yasumasa Nakai, and Kanta Matsuura</i>	
Optimal Authenticated Data Structures with Multilinear Forms .....	246
<i>Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos</i>	

## Point Encoding and Pairing-Friendly Curves

Deterministic Encoding and Hashing to Odd Hyperelliptic Curves .....	265
<i>Pierre-Alain Fouque and Mehdi Tibouchi</i>	
Encoding Points on Hyperelliptic Curves over Finite Fields in Deterministic Polynomial Time .....	278
<i>Jean-Gabriel Kammerer, Reynald Lercier, and Guénaél Renault</i>	
A New Method for Constructing Pairing-Friendly Abelian Surfaces .....	298
<i>Robert Drylo</i>	

Generating More Kawazoe-Takahashi Genus 2 Pairing-Friendly Hyperelliptic Curves . . . . .	312
<i>Ezekiel J. Kachisa</i>	

## ID-Based Encryption Schemes

New Identity-Based Proxy Re-encryption Schemes to Prevent Collusion Attacks . . . . .	327
<i>Lihua Wang, Licheng Wang, Masahiro Mambo, and Eiji Okamoto</i>	
Fully Secure Anonymous HIBE and Secret-Key Anonymous IBE with Short Ciphertexts . . . . .	347
<i>Angelo De Caro, Vincenzo Iovino, and Giuseppe Persiano</i>	
Chosen-Ciphertext Secure Identity-Based Encryption from Computational Bilinear Diffie-Hellman . . . . .	367
<i>David Galindo</i>	

## Invited Talk 3

A Survey of Local and Global Pairings on Elliptic Curves and Abelian Varieties . . . . .	377
<i>Joseph H. Silverman</i>	

## Efficient Hardware, FPGAs, and Algorithms

Compact Hardware for Computing the Tate Pairing over 128-Bit-Security Supersingular Curves . . . . .	397
<i>Nicolas Estibals</i>	
A Variant of Miller's Formula and Algorithm . . . . .	417
<i>John Bozall, Nadia El Mrabet, Fabien Laguillaumie, and Duc-Phong Le</i>	
Pairing Computation on Elliptic Curves with Efficiently Computable Endomorphism and Small Embedding Degree . . . . .	435
<i>Sorina Ionica and Antoine Joux</i>	
High Speed Flexible Pairing Cryptoprocessor on FPGA Platform . . . . .	450
<i>Santosh Ghosh, Debdeep Mukhopadhyay, and Dipanwita Roychowdhury</i>	

<b>Author Index</b> . . . . .	467
-------------------------------	-----