

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

University of Dortmund, 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 of Computer Science, Saarbruecken, Germany

Hovav Shacham Brent Waters (Eds.)

Pairing-Based Cryptography – Pairing 2009

Third International Conference
Palo Alto, CA, USA, August 12-14, 2009
Proceedings

Volume Editors

Hovav Shacham
University of California at San Diego
Department of Computer Science and Engineering
9500 Gilman Drive, MC 0404
La Jolla, CA 92093-0404, USA
E-mail: hovav@cs.ucsd.edu

Brent Waters
University of Texas at Austin
Department of Computer Science
1 University Station C0500, Taylor Hall 2.124
Austin, TX 78712-1188, USA
E-mail: bwaters@cs.utexas.edu

Library of Congress Control Number: 2009930958

CR Subject Classification (1998): E.3, D.4.6, F.2.2, G.2, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN	0302-9743
ISBN-10	3-642-03297-4 Springer Berlin Heidelberg New York
ISBN-13	978-3-642-03297-4 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 2009
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12723874 06/3180 5 4 3 2 1 0

Preface

Pairing 2009, the Third International Conference on Pairing-Based Cryptography, was held at Stanford University in Palo Alto during August 12–14, 2009. The conference was sponsored by Voltage Security and Microsoft Corporation. Terence Spies served as General Chair of the Conference and we had the privilege of serving as Program Co-chairs.

The conference received 38 submissions. These were reviewed by a committee of 23 members. The committee had a three-week individual review phase followed by three weeks of discussion. After careful deliberation, the committee chose 16 papers for the Pairing 2009 conference. Detailed reviews were given to the authors, and the authors were given three weeks to submit the final version. These final versions were not subject to external review and the authors bear full responsibility for their contents.

We are delighted to have had three invited speakers for Pairing 2009. Victor Miller spoke on the origins of pairing-based cryptography. His talk was complemented by Tanja Lange’s, who covered the evolution of the mathematics behind pairings and shared recent results. Finally, Amit Sahai spoke on his work (with Jens Groth and Rafi Ostrovksy) realizing non-interactive zero knowledge proofs from pairings. This work has been highly influential and multiple papers accepted at this conference built upon it. In addition, there was a “Hot Topics” session at this conference where we asked several researchers to give 10-minute presentations of recent results.

We would like to thank everyone who contributed to the conference. First, thanks to the members of our Program Committee for their excellent reviews, the difficult decisions they made in a short time, and their conscientious, thorough shepherding. Second, thanks to the Pairing Conference Steering Committee and the Chairs of previous Pairing conferences and workshops. We would like to extend a particular thanks to Steven Galbraith and Kenny Paterson, Program Chairs of Pairing 2008, whose experience and advice were invaluable to us in our planning of this conference. Third, we would like to thank Shai Halevi, whose wonderful Web Submission and Review Software we used and who hosted and administered the submission and review site for us on the IACR’s servers. Fourth, we are grateful for Voltage Security and Microsoft for their generous support. Finally, we are especially indebted to Terence Spies for his service as General Chair. Without him the conference would not have been possible.

August 2009

Hovav Shacham
Brent Waters

Pairing 2009

The Third International Conference on Pairing-Based Cryptography

Stanford, California

August 12–14, 2009

Sponsored by *Voltage Security and Microsoft*

General Chair

Terence Spies

Voltage Security

Program Chairs

Hovav Shacham

UC San Diego, USA

Brent Waters

UT Austin, USA

Program Committee

Michel Abdalla

École Normale Supérieure, France

Paulo Barreto

University of São Paulo, Brazil

Xavier Boyen

Stanford, USA

Melissa Chase

Microsoft Research, USA

David Mandell Freeman

CWI; Universiteit Leiden, The Netherlands

Steven Galbraith

Royal Holloway, University of London, UK

Pierrick Gaudry

CNRS, INRIA, Nancy Université, France

Matthew Green

Johns Hopkins, USA

Jens Groth

University College London, UK

Florian Hess

TU Berlin, Germany

Tanja Lange

TU Eindhoven, The Netherlands

Kristin Lauter

Microsoft Research, USA

Gregory Neven

IBM Zurich Research Laboratory, Switzerland

Tatsuaki Okamoto

NTT, Japan

Dan Page

University of Bristol, UK

Kenny Paterson

Royal Holloway, University of London, UK

Michael Scott

Dublin City University, Ireland

Hovav Shacham

UC San Diego, USA

Elaine Shi

PARC, USA

Nigel Smart

University of Bristol, UK

Tsuyoshi Takagi

Future University Hakodate, Japan

Fré Vercauteren

KU Leuven, Belgium

Brent Waters

UT Austin, USA

External Reviewers

John Bethencourt
Sébastien Canard
Scott E. Coull
Yuto Kawahara
Benoît Libert
Mark Manulis

Atsuko Miyaji
Peter Montgomery
Yasuyuki Nogami
Pascal Paillier
Emily Shen
Masaaki Shirase

Katsuyuki Takashima
Damien Vergnaud
Ali Zandi

Table of Contents

Signature Security

Boneh-Boyen Signatures and the Strong Diffie-Hellman Problem	1
<i>David Jao and Kayo Yoshida</i>	
Security of Verifiably Encrypted Signatures and a Construction without Random Oracles	17
<i>Markus Rückert and Dominique Schröder</i>	
Multisignatures as Secure as the Diffie-Hellman Problem in the Plain Public-Key Model	35
<i>Duc-Phong Le, Alexis Bonnet, and Alban Gabillon</i>	

Curves

On the Security of Pairing-Friendly Abelian Varieties over Non-prime Fields	52
<i>Naomi Benger, Manuel Charlemagne, and David Mandell Freeman</i>	
Generating Pairing-Friendly Curves with the CM Equation of Degree 1	66
<i>Hyang-Sook Lee and Cheol-Min Park</i>	

Pairing Computation

On the Final Exponentiation for Calculating Pairings on Ordinary Elliptic Curves	78
<i>Michael Scott, Naomi Benger, Manuel Charlemagne, Luis J. Dominguez Perez, and Ezekiel J. Kachisa</i>	
Faster Pairings on Special Weierstrass Curves	89
<i>Craig Costello, Huseyin Hisil, Colin Boyd, Juan Gonzalez Nieto, and Kenneth Koon-Ho Wong</i>	
Fast Hashing to G_2 on Pairing-Friendly Curves	102
<i>Michael Scott, Naomi Benger, Manuel Charlemagne, Luis J. Dominguez Perez, and Ezekiel J. Kachisa</i>	

NIZKs and Applications

Compact E-Cash and Simulatable VRFs Revisited	114
<i>Mira Belenkiy, Melissa Chase, Markulf Kohlweiss, and Anna Lysyanskaya</i>	

Proofs on Encrypted Values in Bilinear Groups and an Application to Anonymity of Signatures	132
<i>Georg Fuchsbauer and David Pointcheval</i>	

Group Signatures

Identity Based Group Signatures from Hierarchical Identity-Based Encryption	150
<i>Nigel P. Smart and Bogdan Warinschi</i>	
Forward-Secure Group Signatures from Pairings	171
<i>Toru Nakanishi, Yuta Hira, and Nobuo Funabiki</i>	
Efficient Traceable Signatures in the Standard Model	187
<i>Benoît Libert and Moti Yung</i>	

Protocols

Strongly Secure Certificateless Key Agreement	206
<i>Georg Lippold, Colin Boyd, and Juan Gonzalez Nieto</i>	
Universally Composable Adaptive Priced Oblivious Transfer	231
<i>Alfredo Rial, Markulf Kohlweiss, and Bart Preneel</i>	
Conjunctive Broadcast and Attribute-Based Encryption	248
<i>Nuttapong Attrapadung and Hideki Imai</i>	

Author Index	267
-------------------------------	-----