

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

Zhenfu Cao Fangguo Zhang (Eds.)

Pairing-Based Cryptography – Pairing 2013

6th International Conference
Beijing, China, November 22-24, 2013
Revised Selected Papers

Volume Editors

Zhenfu Cao
Shanghai Jiao Tong University
School of Electronic Information and Electrical Engineering
No. 800, Dongchuan Road, Shanghai 200240, China
E-mail: zfcdo@cs.sjtu.edu.cn

Fangguo Zhang
Sun Yat-sen University
School of Information Science and Technology
No. 135, Xingang Xi Road, Guangzhou 510275, China
E-mail: isszhfg@mail.sysu.edu.cn

ISSN 0302-9743
ISBN 978-3-319-04872-7
DOI 10.1007/978-3-319-04873-4
Springer Cham Heidelberg New York Dordrecht London

e-ISSN 1611-3349
e-ISBN 978-3-319-04873-4

Library of Congress Control Number: 2014930884

CR Subject Classification (1998): E.3, K.6.5, D.4.6, E.4, F.2.0, I.1

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer International Publishing Switzerland 2014

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The 6th International Conference on Pairing-Based Cryptography (Pairing 2013) was held in Beijing, China, during November 22–24, 2013. The conference was organized by the Information Security Center of Beijing University of Posts and Telecommunications (BUPT) and the Chinese Association for Cryptologic Research (CACR). The general chairs of the conference were Yixian Yang and Xuejia Lai, and secretarial support was provided by Min Lei from Beijing University of Posts and Telecommunications. We thank both Yixian Yang and Xuejia Lai for their constant efforts and for making this conference possible.

The goal of Pairing 2013 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 59 submissions from 15 countries, out of which 14 papers from 10 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.

Furthermore, the conference featured three invited speakers: Pierrick Gaudry from LORIA, France, Francisco Rodriguez-Henriquez from CINVESTAV-IPN, Mexico, and Xu Maozhi from Peking University, China, whose lectures on cutting-edge research areas — “Computing Discrete Logarithms in Finite Fields of Small Characteristic,” “Implementing Pairing-Based Protocols,” and “Using Endomorphisms to Accelerate Scalar Multiplication,” respectively — contributed in a significant part to the richness of the program. In addition, the program included tutorial talks by Robert H. Deng from Singapore Management University and Peter Schwabe from Radboud University Nijmegen, The Netherlands.

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.

November 2013

Zhenfu Cao
Fangguo Zhang

Organization

Honorary Chair

Dingyi Pei	Guangzhou University
------------	----------------------

General Chairs

Yixian Yang	Beijing University of Posts and Telecommunications
Xuejia Lai	Shanghai Jiao Tong University

Technical Program Committee Co-chairs

Zhenfu Cao	Shanghai Jiao Tong University
Fanguo Zhang	Sun Yat-sen University

Organizing Committee

Qun Luo	Beijing University of Posts and Telecommunications
Licheng Wang	Beijing University of Posts and Telecommunications

Organizing Secretary

Min Lei	Beijing University of Posts and Telecommunications
---------	---

Technical Program Committee

Diego Aranha	University of Brasília, Brazil
Paulo S.L.M. Barreto	University of São Paulo, Brazil
Liqun Chen	Hewlett-Packard Laboratories, UK
Xiaofeng Chen	Xidian University, China
Jérémie Detrey	Inria, France
Xiaolei Dong	Shanghai Jiao Tong University, China
Sylvain Duquesne	Université Rennes, France
Junfeng Fan	K.U. Leuven, Belgium
Dario Fiore	MPI-SWS, Germany
Steven Galbraith	University of Auckland, New Zealand
Sorina Ionica	ENS Paris, France

VIII Organization

Kwangjo Kim
Tanja Lange

Jin Li
Shengli Liu
Sarah Meiklejohn
Atsuko Miyaji
Takeshi Okamoto
Haifeng Qian
Jacob Schuldt
Peter Schwabe
Michael Scott
Jun Shao
Alice Silverberg
Tsuyoshi Takagi
Katsuyuki Takashima
Mehdi Tibouchi
Damien Vergnaud
Baocang Wang
Lihua Wang
Jian Weng
Zhenfeng Zhang
Chang-An Zhao

KAIST, Korea
Technische Universiteit Eindhoven,
The Netherlands
Guangzhou University, China
Shanghai Jiao Tong University, China
University of California, USA
JAIST, Japan
University of Tsukuba, Japan
East China Normal University, China
Royal Holloway, UK
Academia Sinica, Taiwan
Certivox Ltd., UK
Zhejiang Gongshang University, China
U.C. Irvine, USA
Kyushu University, Japan
Mitsubishi Electric, Japan
NIT Secure Platform Laboratories, Japan
École Normale Supérieure, France
Xidian University, China
NICT, Japan
Jinan University, China
Chinese Academy of Sciences, China
Sun Yat-sen University, China

External Reviewers

Razvan Barbulescu
Daniel J. Bernstein
Olivier Blazy
Angelo De Caro
Jie Chen
Shan Chen
Craig Costello
Keita Emura
Emmanuel Fouotsa
Yuichi Futa
Martin Gagne
Chaowen Guan
Aurore Guillevic
Shuai Han
Mitsuhiro Hattori
Kenichiro Hayasaka
Takuya Hayashi
Kai He
Zhengan Huang

Tao Jiang
Naoki Kanayama
Yutaka Kawai
Thorsten Kleinjung
Liang Liu
Francois Morain
Michael Naehrig
Takashi Nishide
Baodong Qin
Elizabeth Quaglia
Chunhua Su
Satoru Tanaka
Christophe Tran
Jianfeng Wang
Hongfeng Wu
Shota Yamada
Takanori Yasuda

Table of Contents

EAGL: An Elliptic Curve Arithmetic GPU-Based Library for Bilinear Pairing	1
<i>Shi Pu and Jyh-Charn Liu</i>	
Weakness of $\mathbb{F}_{3^{6 \cdot 509}}$ for Discrete Logarithm Cryptography	20
<i>Gora Adj, Alfred Menezes, Thomaz Oliveira, and Francisco Rodríguez-Henríquez</i>	
The Special Number Field Sieve in \mathbb{F}_{p^n} : Application to Pairing-Friendly Constructions	45
<i>Antoine Joux and Cécile Pierrot</i>	
Efficient Semi-static Secure Broadcast Encryption Scheme	62
<i>Jongkil Kim, Willy Susilo, Man Ho Au, and Jennifer Seberry</i>	
Pairing Inversion via Non-degenerate Auxiliary Pairings	77
<i>Seunghwan Chang, Hoon Hong, Eunjeong Lee, and Hyang-Sook Lee</i>	
Constructing Symmetric Pairings over Supersingular Elliptic Curves with Embedding Degree Three	97
<i>Tadanori Teruya, Kazutaka Saito, Naoki Kanayama, Yuto Kawahara, Tetsutaro Kobayashi, and Eiji Okamoto</i>	
Predicate- and Attribute-Hiding Inner Product Encryption in a Public Key Setting	113
<i>Yutaka Kawai and Katsuyuki Takashima</i>	
Fast Symmetric Pairing Revisited	131
<i>Xusheng Zhang and Kunpeng Wang</i>	
Efficient Leakage-Resilient Identity-Based Encryption with CCA Security	149
<i>Shi-Feng Sun, Dawu Gu, and Shengli Liu</i>	
Revocable IBE Systems with Almost Constant-Size Key Update	168
<i>Le Su, Hoon Wei Lim, San Ling, and Huaxiong Wang</i>	
Pseudo 8-Sparse Multiplication for Efficient Ate-Based Pairing on Barreto-Naehrig Curve	186
<i>Yuki Mori, Shoichi Akagi, Yasuyuki Nogami, and Masaaki Shirase</i>	
Adaptable Ciphertext-Policy Attribute-Based Encryption	199
<i>Junzuo Lai, Robert H. Deng, Yanjiang Yang, and Jian Weng</i>	

Algorithms for Pairing-Friendly Primes 215
 Maciej Grześkowiak

Panda: Pairings and Arithmetic 229
 *Chitchanok Chuengsatiansup, Michael Naehrig, Pance Ribarski, and
 Peter Schwabe*

Author Index 251