Lecture Notes in Computer Science 8365

Zhenfu Cao   Fangguo Zhang (Eds.)

Pairing-Based Cryptography – Pairing 2013

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

Springer

Volume Editors

Zhenfu Cao
Shanghai Jiao Tong University
School of Electronic Information and Electrical Engineering
No. 800, Dongchuan Road, Shanghai 200240, China
E-mail: zfcao@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 e-ISSN 1611-3349
ISBN 978-3-319-04872-7 e-ISBN 978-3-319-04873-4
DOI 10.1007/978-3-319-04873-4
Springer Cham Heidelberg New York Dordrecht London

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

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 form 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
Fangguo 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

Kwangjo Kim	KAIST, Korea
Tanja Lange	Technische Universiteit Eindhoven, The Netherlands
Jin Li	Guangzhou Universtiy, China
Shengli Liu	Shanghai Jiao Tong University, China
Sarah Meiklejohn	University of California, USA
Atsuko Miyaji	JAIST, Japan
Takeshi Okamoto	University of Tsukuba, Japan
Haifeng Qian	East China Normal University, China
Jacob Schuldt	Royal Holloway, UK
Peter Schwabe	Academia Sinica, Taiwan
Michael Scott	Certivox Ltd., UK
Jun Shao	Zhejiang Gongshang University, China
Alice Silverberg	U.C. Irvine, USA
Tsuyoshi Takagi	Kyushu University, Japan
Katsuyuki Takashima	Mitsubishi Electric, Japan
Mehdi Tibouchi	NIT Secure Platform Laboratories, Japan
Damien Vergnaud	École Normale Supérieur, France
Baocang Wang	Xidian University, China
Lihua Wang	NICT, Japan
Jian Weng	Jinan University, China
Zhenfeng Zhang	Chinese Academy of Sciences, China
Chang-An Zhao	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