Lecture Notes in Computer Science 4575

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

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
Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos
University of California, Los Angeles, CA, USA

Doug Tygar
University of California, Berkeley, CA, USA

Moshe Y. Vardi
Rice University, Houston, TX, USA

Gerhard Weikum
Max-Planck Institute of Computer Science, Saarbruecken, Germany

Tsuyoshi Takagi Tatsuaki Okamoto
Eiji Okamoto Takeshi Okamoto (Eds.)

Pairing-Based Cryptography – Pairing 2007

First International Conference
Tokyo, Japan, July 2-4, 2007
Proceedings

Springer

Volume Editors

Tsuyoshi Takagi
Future University Hakodate, Japan
E-mail: takagi@fun.ac.jp

Tatsuaki Okamoto
NTT Laboratories, Nippon Telegraph and Telephone Corporation, Yokosuka, Japan
E-mail: okamoto.tatsuaki@lab.ntt.co.jp

Eiji Okamoto
University of Tsukuba, Japan
E-mail: okamoto@risk.tsukuba.ac.jp

Takeshi Okamoto
University of Tsukuba, Japan
E-mail: ken@risk.tsukuba.ac.jp

Library of Congress Control Number: 2007929851

CR Subject Classification (1998): E.3, D.4.6, F.2.1-2, G.2, K.6.5, C.2

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-73488-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-73488-8 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 is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2007
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12087259 06/3180 5 4 3 2 1 0

Preface

The 1st International Conference on Pairing-Based Cryptography (Pairing 2007) was held in Tokyo, Japan, during July 2–4, 2007. Pairing-based cryptography has been causing a paradigm shift in cryptography–an ever increasing number of novel protocols using pairing have been appearing in the literature: identity-based encryption, short signature, and efficient broadcast encryption, to mention but a few. The aim of Pairing 2007 was to bring together leading researchers and practitioners from academia and industry, all concerned with problems related to pairing-based cryptography. This conference was sponsored by the University of Tsukuba, and it was offered in cooperation with Tokyo Section, The Institute of Electrical and Electronics Engineers (IEEE) and The Japan Society for Industrial and Applied Mathematics (JSIAM).

Pairing 2007 received 86 submissions from all over the world. Each paper was double-blindly evaluated by at least three reviewers regarding the technical relevance to pairing-based cryptography, and 18 papers were selected for presentation at Pairing 2007. We would like to thank all members of the Program Committee for their support and enormous investment of time throughout the whole delicate review process. We are also extremely grateful for all the help and support of a large number of external reviewers who reviewed submissions in their area of expertise.

The program also included five invited talks by Dan Boneh from Stanford University, USA; Steven Galbraith from Royal Holloway University of London, UK; Alfred Menezes from University of Waterloo, Canada; Takakazu Satoh from Tokyo Institute of Technology, Japan; and Michael Scott from Dublin City University, Ireland. At least one page of the extended abstract for each invited talk is included in the proceedings.

We would like to thank all the members of the Organizing Committee for their work in the publication and organization of Pairing 2007. The review server and its backup system unexpectedly went out of service, and the review process had to be restarted from scratch. We gratefully thank Atsuo Inomata and Akira Kanaoka for their enormous support in installing and operating the iChair system during the review process. Again, we gratefully appreciate the patient effort of all reviewers, especially in light of the server accident.

Finally, we would like to thank all the authors who submitted papers to Pairing 2007.

April 2007

Tsuyoshi Takagi
Tatsuaki Okamoto
Eiji Okamoto
Takeshi Okamoto

Pairing 2007

The First International Conference on Pairing-Based Cryptography

Tokyo, Japan, July 2–4, 2007

Sponsored by the *University of Tsukuba*, *IEEE Tokyo Section*, and *The Japan Society for Industrial and Applied Mathematics (JSIAM)*.

General Co-chairs

Eiji Okamoto, University of Tsukuba, Japan
Takeshi Okamoto, University of Tsukuba, Japan

Program Co-chairs

Tsuyoshi Takagi, Future University Hakodate, Japan
Tatsuaki Okamoto, NTT, Japan

Organizing Co-chairs

Hiroshi Doi, Institute of Information Security, Japan
Atsuo Inomata, Japan Science and Technology Agency, Japan
Akira Kanaoka, University of Tsukuba, Japan
Masahiro Mambo, University of Tsukuba, Japan

Program Committee

Paulo Barreto, University of Sao Paulo, Brazil
Johannes Buchmann, Technische Universität Darmstadt, Germany
Jan Camenisch, IBM Zurich Research Laboratory, Switzerland
Jinhui Chao, Chuo University, Japan
Jean-Sebastien Coron, University of Luxembourg, Luxembourg
Iwan Duursma, University of Illinois at Urbana-Champaign, USA
Andreas Enge, Ecole Polytechnique, France
Jun Furukawa, NEC, Japan
David Galindo, University of Malaga, Spain

Goichiro Hanaoka, AIST, Japan
Tetsuya Izu, Fujitsu, Japan
Michael Jacobson, University of Calgary, Canada
Antoine Joux, DGA and Universite de Versailles, France
Marc Joye, Thomson R&D, France
Kwangjo Kim, Information and Communications University, Korea
Tetsutaro Kobayashi, NTT, Japan
Soonhak Kwon, Sungkyunkwan University, Korea
Tanja Lange, Technische Universiteit Eindhoven, The Netherlands
Hyang-Sook Lee, Ewha Womans University, Korea
Atsuko Miyaji, JAIST, Japan
Dan Page, University of Bristol, UK
Jean-Jacques Quisquater, Universite catholique de Louvain, Belgium
Ryuichi Sakai, Osaka Electro-Communication University, Japan
Palash Sarkar, Indian Statistical Institute, India
Igor Shparlinski, Macquarie University, Australia
Nigel Smart, University of Bristol, UK
Willy Susilo, University of Wollongong, Australia
Routo Terada, University of Sao Paulo, Brazil
Shigenori Uchiyama, Tokyo Metropolitan University, Japan
Guilin Wang, Institute for Infocomm Research, Singapore
Victor Wei, Chinese University of Hong Kong, China
Moti Yung, RSA Labs and Columbia University, USA
Fangguo Zhang, Sun Yat-sen University, China

External Reviewers

Nuttapong Attrapadung
Kazumaro Aoki
Joonsang Baek
Daniel J. Bernstein
Jean-Luc Beuchat
Reinier Broker
Sanjit Chatterjee
Xiaofeng Chen
Jung Hee Cheon
Benoit Chevallier-Mames
Sherman S. M. Chow
Thomas Heide Clausen
Yang Cui
Yevgeniy Dodis
Hiroshi Doi
Dang Nguyen Duc
David Freeman
Toshinori Fukunaga
Steven Galbraith
DongGuk Han
Colm O hEigeartaigh
Laura Hitt
Fumitaka Hoshino
Xinyi Huang
Heng Swee Huay
Toshiyuki Issiki
Naoki Kanayama
Aggelos Kiayias
Yongdae Kim
Hirotsugu Kinoshita
Yuichi Komano
Noboru Kunihiro
Soonhak Kwon
Taekyoung Kwon
Dong Hoon Lee
Eunjeng Lee
Hyunrok Lee
Taekyoung Lee
Yoonjin Lee
Benoit Libert
Vo Duc Liem
Joseph K. Liu
Kazuto Matsuo
Maria Meyerovich
Michael Naehrig
Koh-ichi Nagao
Toshiya Nakajima
Gregory Neven
Keiichiro Nishimoto
Wakaha Ogata
Sunsuke Ohta
Takao Okubo
Akira Otsuka
Jehong Park

Young-Ho Park
Pieter Rozenhart
Eun-Kyung Ryu
Taiichi Saito
Abhi Shelat
Alan Silvester
Kyungah Shim
SeongHan Shin
Mike Scott
Martijn Stam
Koutarou Suzuki
Katsuyuki Takashima
Masahiko Takenaka
Satoru Tanaka
Adrian Tang
Mark Velichka
Jonathan Webster
Rui Zhang

Table of Contents

Invited Talk I

Bilinear Groups of Composite Order 1
Dan Boneh

Applications

Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System 2
Yong Ho Hwang and Pil Joong Lee

Practical Time Capsule Signatures in the Standard Model from Bilinear Maps 23
Benoît Libert and Jean-Jacques Quisquater

Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys 39
Cécile Delerablée, Pascal Paillier, and David Pointcheval

Certificateless Public Key Encryption

Certificateless Public Key Encryption in the Selective-ID Security Model 60
Jong Hwan Park, Kyu Young Choi, Jung Yeon Hwang, and Dong Hoon Lee

General and Efficient Certificateless Public Key Encryption Constructions 83
Zhaohui Cheng, Liqun Chen, Li Ling, and Richard Comley

Invited Talk II

Hyperelliptic Pairings 108
Steven D. Galbraith, Florian Hess, and Frederik Vercauteren

Hyperelliptic Curves

Zeta Function and Cryptographic Exponent of Supersingular Curves of Genus 2 132
Gabriel Cardona and Enric Nart

Constructing Pairing-Friendly Genus 2 Curves with Ordinary Jacobians 152
David Freeman

Invited Talk III

Implementing Cryptographic Pairings 177
Michael Scott

Implementation

Implementing Cryptographic Pairings over Barreto-Naehrig Curves 197
Augusto Jun Devegili, Michael Scott, and Ricardo Dahab

Instruction Set Extensions for Pairing-Based Cryptography 208
Tobias Vejda, Dan Page, and Johann Großschädl

The Importance of the Final Exponentiation in Pairings When Considering Fault Attacks 225
Claire Whelan and Michael Scott

Protocol I

Proxy Re-encryption Systems for Identity-Based Encryption 247
Toshihiko Matsuo

Fair Blind Signatures Revisited 268
Emeline Hufschmitt and Jacques Traoré

Invited Talk IV

Supersingular Elliptic Curves in Cryptography 293
Alfred Menezes

Analysis

On the Minimal Embedding Field 294
Laura Hitt

Remarks on Cheon's Algorithms for Pairing-Related Problems 302
Shunji Kozaki, Taketeru Kutsuma, and Kazuto Matsuo

Invited Talk V

On Pairing Inversion Problems 317
Takakazu Satoh

Algorithms

The Tate Pairing Via Elliptic Nets 329
Katherine E. Stange

Eta Pairing Computation on General Divisors over Hyperelliptic Curves $y^2 = x^7 - x \pm 1$ 349
Eunjeong Lee, Hyang-Sook Lee, and Yoonjin Lee

Protocol II

Provably Secure Pairing-Based Convertible Undeniable Signature with Short Signature Length 367
Xinyi Huang, Yi Mu, Willy Susilo, and Wei Wu

Identity-Based Encryption: How to Decrypt Multiple Ciphertexts Using a Single Decryption Key 392
Fuchun Guo, Yi Mu, and Zhide Chen

Author Index 407