

# Call for Participation

## Pairing 2007

July 2-4, 2007, Tokyo, Japan



The First International Conference on Pairing-based Cryptography (Pairing 2007) will be held in Tokyo, Japan on July 2-4, 2007. Please refer to <http://www.pairing-conference.org/> for further details.

### Scope

Since the introduction of pairings in constructive cryptographic applications, an ever increasing number of protocols have been appearing in the literature: identity-based encryption, short signature, and efficient broadcast encryption to mention but a few. An appropriate mix of theoretical foundations and practical considerations is essential to fully exploit the possibilities offered by pairings: number theory, cryptographic protocols, software and hardware implementations, new security applications, etc.

The aim of "Pairing 2007" is thus 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 will enhance communication among specialists from various research areas and promote creative interdisciplinary collaborations.

Authors are invited to submit papers describing their original research on all aspects of pairing-based cryptography, including, but not limited to the following topics:

#### Area I: Novel cryptographic protocols

- ID-based cryptosystem
- Broadcast encryption
- Authenticated encryption
- Short signature
- Multi or aggregate signature
- Ring, group or threshold signature
- Designed confirmer or undeniable signature
- Blind or partially blind signature
- Identification scheme
- Password authentication system
- Key agreement protocol
- Provably secure protocol

#### Area II: Mathematical foundation

- Weil, Tate, Eta, and Ate pairings
- Security consideration of pairing
- Pairings on Abelian variety
- Generation of pairing friendly curves
- (Hyper-) Elliptic curve cryptosystem
- Point counting algorithm
- Number theoretic algorithms
- Addition formula on the divisor group

#### Area III: SW/HW implementation

- Secure operating system
- Efficient software implementation
- FPGA or ASIC implementation
- Smart card implementation
- RFID security
- Middleware security
- Side channel attack
- Fault attack

#### Area IV: Applied security

- Novel security applications
- Secure ubiquitous computing
- Security management
- PKI model
- Application to network security
- Grid computing
- Internet and web security
- E-business or E-commerce security

### Invited Talks

Dan Boneh, Stanford University, USA

Steven Galbraith, Royal Holloway University of London, UK

Alfred Menezes, University of Waterloo, Canada

Takakazu Satoh, Tokyo Institute of Technology, Japan

Michael Scott, Dublin City University, Ireland

## General Chairs

Eiji Okamoto, University of Tsukuba, Japan

Takeshi Okamoto, University of Tsukuba, Japan

## Program Chairs

Tsuyoshi Takagi, Future University Hakodate, Japan

Tatsuaki Okamoto, NTT, Japan

## Program Committee

Paulo Barreto, University of Sao Paulo, Brazil

Johannes Buchmann, Technische Universitat 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, 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

## Sponsors

The conference is hosted by University of Tsukuba. It is offered in cooperation with IEEE Tokyo Section and the Japan Society for Industrial and Applied Mathematics (JSIAM).

## Proceedings

The conference proceedings of Pairing 2007 will be published in the Lecture Notes in Computer Science series by Springer Verlag.

## Contact

If you have any questions, please contact: [info@pairing.jp](mailto:info@pairing.jp).