

Call for Participation

Pairing 2008



The Second International Conference on Pairing-based Cryptography (Pairing 2008) will be held at Royal Holloway, University of London, UK in September 1-3, 2008. Please refer to <http://www.pairing-conference.org/> for further details.

Motivation and Scope

Pairing-based cryptography is an extremely active area of research which has allowed elegant solutions to a number of long-standing open problems in cryptography (such as efficient identity-based encryption). New developments continue to be made at a rapid pace.

To fully exploit the possibilities offered by pairings it is necessary to have an appropriate background in several theoretical and practical areas. In particular, the development of pairing based cryptography has been both driven and influenced by developments in number theory, algebraic geometry, cryptographic protocols, software and hardware implementations, new security applications, etc.

The aim of "Pairing" conference is thus to bring together leading researchers and practitioners from academia and industry, all concerned with problems related to pairing-based cryptography. The first conference Pairing 2007 was held in Japan and the proceedings were published in Springer LNCS 4575. We hope that this conference will enhance communication among specialists from various research areas and promote creative interdisciplinary collaboration

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 and certificateless cryptosystems
- Broadcast encryption, signcryption etc
- Short/multi/aggregate/group/ring/threshold /blind signatures
- Designed confirmer or undeniable signature
- Identification /authentication schemes
- Key agreement

Area II: Mathematical foundations

- Efficient Weil and Tate variants
- Security consideration of pairings
- Other pairings and applications of pairings in mathematics
- Generation of pairing friendly curves
- Elliptic and hyperelliptic curves
- Number theoretic algorithms
- Addition formula on the divisor group

Area III: SW/HW implementation

- Secure operating systems
- Efficient software implementation
- FPGA or ASIC implementation
- Smart card implementation
- RFID security
- Middleware security
- Side channel and fault attacks

Area IV: Applied security

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

Invited Speakers

Xavier Boyen (Voltage, USA)

Nigel Smart (University of Bristol, UK)

Florian Hess (TU Berlin, Germany)

General Chairs

Steven Galbraith, Royal Holloway, UK
Takeshi Okamoto, Tsukuba University of Technology, Japan

Kenny Paterson, Royal Holloway, UK

Program Committee

Paulo Barreto, University of Sao Paulo, Brazil
Jan Camenisch, IBM Zurich Research Laboratory, Switzerland
Liqun Chen, Hewlett-Packard labs, UK
Andreas Enge, Ecole polytechnique, France
Steven Galbraith, Royal Holloway, UK (co-chair)
David Galindo, University of Malaga, Spain
Marc Joye, Thomson R&D, France
Eike Kiltz, CWI, Netherlands
Soonhak Kwon, Sungkyunkwan University, Korea
Tanja Lange, Technische Universiteit Eindhoven, Netherlands
Kristin Lauter, Microsoft, USA

Alfred Menezes, University of Waterloo, Canada
Eiji Okamoto, University of Tsukuba, Japan
Tatsuaki Okamoto, NTT, Japan
Dan Page, University of Bristol, UK
Kenny Paterson, Royal Holloway, UK (co-chair)
Takakazu Satoh, Tokyo Tech, Japan
Michael Scott, Dublin City University, Ireland
Hovav Shacham, UCSD, USA
Igor Shparlinski, Macquarie University, Australia
Tsuyoshi Takagi, Future University Hakodate, Japan
Frederik Vercauteren, Leuven, Belgium

Sponsors

The conference is sponsored by Voltage Security, The London Mathematical Society and Microsoft Research..

Proceedings

The conference proceedings of Pairing 2008 will be published by Springer in the Lecture Notes in Computer Science series.

Contact

If you have any questions, please contact : info@pairing-conference.org.