- Call for Participation -

The 4th International Conference on

Pairing-based Cryptography (Pairing 2010)

December 13-15, 2010

Yamanaka Onsen (Hot Spring), Ishikawa, Japan

Web Page: http://www.pairing-conference.org/ Contact: pairing2010-info@m.aist.go.jp

Overview

The focus of Pairing 2010 is on all aspects of pairing-based cryptography, including: cryptographic primitives and protocols, mathematical foundations, software and hardware implementation, and applied security. The first International Conference on Pairing-based Cryptography (Pairing 2007) was held in Tokyo, Japan, followed by Egham, UK in 2008, and Palo Alto, USA in 2009. The next conference (Pairing 2010) will be held in Yamanaka Onsen (Hot Spring), Japan on December 13-15, 2010. For further information about the conference, visit http://www.pairing-conference.org/.

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. The proceedings of Pairing 2007, 2008, and 2009 were published in Springer's LNCS 4575, 5209, and 5671, respectively. We hope that this conference will enhance communication among specialists from various research areas and promote creative interdisciplinary collaboration. We received a lot of papers describing research on all aspects of pairing-based cryptography, including, but not limited to the topics listed below. Selected papers through a rigorous review process among them will be announced soon. We now solicit you to attend Pairing 2010. Please check the website for more information.

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
- Number theoretic algorithms
- Generation of pairing friendly curves
- Elliptic and hyperelliptic curves
- Addition formula on the divisor group
- Other pairings and applications of pairings in mathematics

Area III: SW/HW implementation

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

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
- Cloud computing
- Mobile and wireless network security
- Application to sensor network security
- Peer-to-peer security

Invited Speakers

Title: Pairing-based non-interactive zero-knowledge proofs	Speaker: Jens Groth (UCL, UK)
Title: A survey of local and global pairings on elliptic curves and abelian varieties	Speaker: Joseph H. Silverman (Brown University, USA)
Title: Some security topics with possible applications for pairing-based cryptography	Speaker: Gene Tsudik (University of California at Irvine, USA)

Conference Venue

Yamanaka Onsen (Hot Spring) was founded 1300 years ago. Magnificent natural sceneries and traditional cultures are still well-preserved in the area. For more information, visit http://www.yamanaka-spa.or.jp/english/welcome/index.html.

Special Attractions in banquet

You can enjoy eating and drinking Japanese food, watching "Noh" and "Kyogen". Noh and Kyogen are one category of "Nogaku", which is one of the traditional Japanese theatrical arts. The Japanese Government designated Nogaku as an Important Intangible Cultural Property in 1957. Nogaku was designated by UNESCO as World Intangible Cultural Heritage in 2001.

Committee and Organizers

Jointly Organized By:

National Institute of Advanced Industrial Science and Technology (AIST), Japan
Japan Advanced Institute of Science and Technology (JAIST), Japan

Supported By:

Technical Committee on Information and Communication System Security (ICSS), IEICE, Japan
Technical Committee on Information Security (ISEC), IEICE, Japan
Special Interest Group on Computer Security (CSEC), IPSJ, Japan

Sponsored By:

National Institute of Information and Communications Technology (NICT)
Microsoft Research
Voltage Security
Hitachi, Ltd

General Chair:

Akira Otsuka	*AIST, Japan*

Program Co-Chairs:

Marc Joye	*Technicolor, France*
Atsuko Miyaji	*JAIST, Japan*

Organizing Committee:

Tomoyuki Asano	*Sony, Japan*
Nuttapong Attrapadung	*AIST, Japan*
Hiroshi Doi	*IISEC, Japan*
Goichiro Hanaoka	*AIST, Japan*
Mitsuhiro Hattori	*Mitsubishi Electric, Japan*
Shoichi Hirose	*University of Fukui, Japan*
Masaki Inamura	*KDDI R&D Labs Inc., Japan*
Atsuo Inomata	*NAIST, Japan*
Yasuharu Katsuno	*IBM Research - Tokyo, Japan*
Tetsutaro Kobayashi	*NTT Labs, Japan*
Toshihiko Matsuo	*NTT Data, Japan*
Natsume Matsuzaki	*Panasonic, Japan*
Hideyuki Miyake	*Toshiba, Japan*
Ryo Nojima	*NICT, Japan*
Takeshi Okamoto	*Tsukuba U. of Technology, Japan*
Katsuyuki Okeya	*Hitachi, Japan*
Kazumasa Omote	*JAIST, Japan*
Yuji Suga	*IIJ, Japan*
Tsuyoshi Takagi	*Kyushu University, Japan*
Dai Yamamoto	*Fujitsu Laboratories, Japan*
Toshihiro Yamauchi	*Okayama University, Japan*
Shoko Yonezawa	*AIST, Japan*

Program Committee:

Michel Abdalla	*Ecole Normale Supérieure, France*
Paulo S.L.M. Barreto	*University of São Paulo, Brazil*
Daniel Bernstein	*University of Chicago, USA*
Jean-Luc Beuchat	*Tsukuba Univ., Japan*
Xavier Boyen	*Université de Liège, Belgium*
Ee-Chien Chang	*National Univ. of Singapore, Singapore*
Liqun Chen	*HP Labs, UK*
Reza Rezaeian Farashahi	*Macquarie University, Australia*
David Mandell Freeman	*Stanford University, USA*
Jun Furukawa	*NEC Corporation, Japan*
Craig Gentry	*IBM Research, USA*
Juan González Nieto	*Queensland U. Technology, Australia*
Vipul Goyal	*Microsoft Research, India*
Shai Halevi	*IBM Research, USA*
Antoine Joux	*U. Versailles & DGA, France*
Jonathan Katz	*University of Maryland, USA*
Kwangjo Kim	*KAIST, Korea*
Kristin Lauter	*Microsoft Research, USA*
Pil Joong Lee	*Pohang U. Science and Tech., Korea*
Reynald Lercier	*DGA/CELAR & U. Rennes 1, France*
Benoît Libert	*Univ. Catholique de Louvain, Belgium*
Mark Manulis	*TU Darmstadt, Germany*
Giuseppe Persiano	*Università di Salerno, Italy*
C. Pandu Rangan	*IIT Madras, India*
Christophe Ritzenthaler	*IML, France*
German Saez	*UPC, Spain*
Michael Scott	*Dublin City University, Ireland*
Alice Silverberg	*University of California at Irvine, USA*
Katsuyuki Takashima	*Mitsubishi Electric, Japan*
Keisuke Tanaka	*Tokyo Institute of Technology, Japan*
Edlyn Teske	*University of Waterloo, Canada*
Frederik Vercauteren	*K.U. Leuven, Belgium*
Bogdan Warinschi	*University of Bristol, UK*
Duncan S. Wong	*City University of Hong Kong, China*
Bo-Yin Yang	*Academia Sinica, Taiwan*
Sung-Ming Yen	*National Central University, Taiwan*
Fangguo Zhang	*Sun Yat-sen University, P.R.China*
Jianying Zhou	*I2R, Singapore*