- 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/.

Program

December 13 (Monday)

Session 1 Efficient software implementations (10:10-11:00)

- An Analysis of Affine Coordinates for Pairing Computation *(Kristin Lauter, Peter L. Montgomery & Michael Naehrig)*
- High-Speed Software Implementation of the Optimal Ate Pairing over Barreto-Naehrig Curves *(Jean-Luc Beuchat, Jorge E. Gonzalez-Diaz, Shigeo Mitsunari, Eiji Okamoto, Francisco Rodrriguez-Henriquez & Tadanori Teruya)*

Keynote talk I (11:00-12:00)

- Some Security Topics with Possible Applications for Pairing-Based Cryptography (Gene Tsudik)

Session 2 Digital signatures (14:00-15:15)

- A New Construction of Designated Confirmer Signature and Its Application to Optimistic Fair Exchange *(Qiong Huang, Duncan S. Wong & Willy Susilo)*
- Anonymizable Signature and its Construction from Pairings *(Fumitaka Hoshino, Tetsutaro Kobayashi & Koutarou Suzuki)*
- Identification of Multiple Invalid Pairing-based Signatures in Constrained Batches *(Brian J. Matt)*

Session 3 Cryptographic protocols (15:45-17:00)

- Oblivious Transfer with Access Control: Realizing Disjunction without Duplication *(Ye Zhang, Man Ho Au, Duncan S. Wong, Qiong Huang, Nikos Mamoulis and David W. Cheung & Siu-Ming Yiu)*
- Increased Resilience in Threshold Cryptography: Sharing a Secret with Devices that Cannot Store Shares *(Koen Simoens, Roel Peeters & Bart Preneel)*
- Shorter Verifier-Local Revocation Group Signature with Backward Unlinkability *(Lingbo Wei & Jianwei Liu)*

December 14 (Tuesday)

Session 4 Key agreement (9:15-10:30)

- Strongly Secure Two-Pass Attribute-based Authenticated Key Exchange *(Kazuki Yoneyama)*
- Constructing Certificateless Encryption and ID-Based Encryption from ID-Based Key Agreement *(Dario Fiore, Rosario Gennaro & Nigel P. Smart)*
- Ephemeral Key Leakage Resilient and Efficient ID-AKEs that can Share Identities, Private and Master Keys *(Atsushi Fujioka, Koutarou Suzuki & Berkant Ustaoglu)*

Keynote talk II (11:00-12:00)

Pairing-based Non-interactive Zero-Knowledge Proofs (Jens Groth)

Session 5 Applications (14:00-15:15)

- Designing a Code Generator for Pairing Based Cryptographic Functions *(Luis J. Dominguez Perez & Michael Scott)*
- Efficient Generic Constructions of Timed-Release Encryption with Pre-open Capability *(Takahiro Matsuda, Yasumasa Nakai & Kanta Matsuura)*
- Optimal Authenticated Data Structures with Multilinear Forms *(Charalampos Papamanthou, Roberto Tamassia & Nikos Triandopoulos)*

Session 6 Point encoding & Pairing-friendly curves (15:45-17:25)

- Deterministic Encoding and Hashing to Odd Hyperelliptic Curves *(Pierre-Alain Fouque & Mehdi Tibouchi)*
- Encoding Points on Hyperelliptic Curves over Finite Fields in Deterministic Polynomial Time *(Jean-Gabriel Kammerer, Reynald Lercier & Guénaël Renault)*
- A New Method for Constructing Pairing-Friendly Abelian Surfaces *(Robert Drylo)*
- Generating more Kawazoe-Takahashi Genus 2 Pairing-friendly Hyperelliptic Curves *(Ezekiel J Kachisa)*

December 15 (Wednesday)

Session 7 Identity-based encryption schemes (9:15-10:30)

- New Identity-Based Proxy Re-Encryption Schemes to Prevent Collusion Attacks *(Lihua Wang, Licheng Wang, Masahiro Mambo & Eiji Okamoto)*
- Fully Secure Anonymous HIBE and Secret-Key Anonymous IBE with Short Ciphertexts *(Angelo De Caro, Vincenzo Iovino & Giuseppe Persiano)*
- Chosen-Ciphertext Secure Identity-Based Encryption from Computational Bilinear Diffe-Hellman *(David Galindo)*

Keynote talk III(11:00-12:00)

A Survey of Local and Global Pairings on Elliptic Curves and Abelian Varieties (Joseph H. Silverman)

Session 8 Efficient hardware, FPGAs, and algorithms (13:30-15:10)

- Compact Hardware for Computing the Tate Pairing over 128-bit-security Supersingular Curves *(Nicolas Estibals)*
- A Variant of Miller's Formula and Algorithm *(John Boxall, Nadia El Mrabet, Fabien Laguillaumie & Duc-Phong Le)*
- Pairing Computation on Elliptic Curves with Efficiently Computable Endomorphism and Small Embedding Degree *(Sorina Ionica & Antoine Joux)*
- High Speed Flexible Pairing Cryptoprocessor on FPGA Platform *(Santosh Ghosh, Debdeep Mukhopadhyay & Dipanwita Roy Chowdhury)*

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
.

Registration

- On-line registration: linked from Pairing 2010 web page
- Early fee registration deadline: November 6, 2010

Act quickly!

Registration deadline

- Payment by bank transfer: December 4, 2010
- Payment by credit card: December 4, 2010

Social Events

The conference social events include:

- Lunches at Mugen-an and Basho-no-Yakata Museum
- Banquet with a traditional Japanese cuisine together with locally-brewed sake

Noh

Kyogen

Basho-no-Yakata

Mugen-an

Committee and Organizers

General Chair:

Akira Otsuka	AIST, Japan

Program Co-Chairs

Marc Joye	Technicolor, France
Atsuko Miyaji	JAIST, Japan

Jointly Organized By:

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

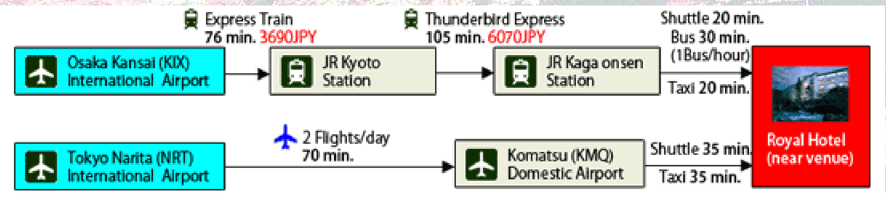
Supported By:

- 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

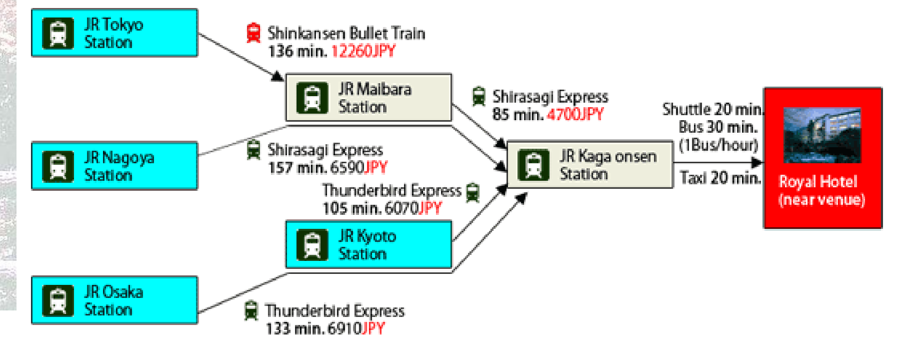
Sponsored By:

- National Institute of Information and Communications Technology
- Microsoft Research
- Voltage Security
- Hitachi, Ltd

From overseas



From domestic areas


JR Tokyo Station
Shinkansen Bullet Train
136 min. 12260JPY
JR Maibara Station
Shirasagi Express
85 min. 4700JPY
JR Nagoya Station
Shirasagi Express
157 min. 6590JPY
Thunderbird Express
105 min. 6070JPY
JR Kyoto Station
JR Kaga onsen Station
Shuttle 20 min.
Bus 30 min.
(1Bus/hour)
Taxi 20 min.
Royal Hotel (near venue)
JR Osaka Station
Thunderbird Express
133 min. 6910JPY