The 2nd ACM Asia Public Key Cryptography Workshop (ASIAPKC 2014)

Affiliated with ACM ASIACCS 2014

June 3rd 2014, Kyoto, Japan

Workshop website: http://www2.nict.go.jp/nsri/arch/asiapkc2014/

Contact E-mail: asiapkc2014@ml.nict.go.jp

Call for Papers

Public key cryptography plays an essential role in ensuring many security properties required in data processing of various kinds. The theme of this workshop is novel public key cryptosystems for solving a wide range of real-life application problems. This workshop solicits original contributions on both applied and theoretical aspects of public key cryptography.

The proceedings will be published by ACM Press and appear in ACM digital library (as with the ACM ASIACCS 2014 and 1st ASIAPKC proceedings). Submitted papers must be no longer than 10 pages excluding references and appendices, and no longer than 12 pages in total. Camera-ready version must be no longer than 10 pages in ACM's standard double-column format.

Topics of interest to the workshop include, but are not limited to:

- Applied public key cryptography for solving emerging application problems
- Provably secure public key primitives and protocols
- Key management
- Privacy-preserving cryptographic computations
- Two-party and multi-party computations
- Homomorphic public key cryptosystems
- Attributed based and functional public key cryptography
- Digital signatures with special properties
- System security properties of public key cryptography (e.g., dealing with key leakage and selective opening attacks)
- Post-quantum public key cryptographs

Important dates:

Submission due:	~~Feb. 10, 2014~~ Feb. 21, 2014
Notification:	~~Mar. 10, 2014~~ Mar. 21, 2014
Proceedings version due:	~~Mar. 24, 2014~~ Apr. 8, 2014
ASIAPKC workshop:	June. 3, 2014

Submission website:

https://www.easychair.org/conferences/?conf=asiapkc2014

Instructions for authors:

Submission must be written in English. Submitted papers must be no longer than 10 pages excluding references and appendices, and no longer than 12 pages in total. Committee members are not obligated to read appendices, and a paper must be intelligible without the appendices. Submitted papers must be in the double-column ACMSIG Proceedings format (http://www.acm.org/sigs/publications/proceedings-templates, both Option 1 and Option 2 on the page are fine) with page numbers marked. No changes to margins, spacing, or font sizes are allowed from those specified by the style file. The workshop reserves the right to request the source files for a submission to verify compliance with these requirements. Submitted papers must be PDF files.

Submitted papers must be appropriately anonymized. No information about author's name should be identifiable from the paper (including abstract, related work, references). When citing one's own previous work, third person should be used. Submitted papers must not substantially overlap papers that have been published or are simultaneously submitted to a journal, conference or workshop. Simultaneous submission of the same work is prohibited. Authors of accepted papers must guarantee that their papers will be presented at the workshop. The Program Committee reserves the right to reject any paper that does not abide by the rules without considering its technical merits.

Program Co-Chairs:

Keita Emura	National Institute of Information and Communications Technology, Japan
Goichiro Hanaoka	National Institute of Advanced Industrial Science and Technology, Japan
Yunlei Zhao	Fudan University, China

Program Committee (More to be added):

Nuttapong Attrapadung	National Institute of Advanced Industrial Science and Technology, Japan
Sherman Chow	Chinese University of Hong Kong, Hong Kong
Keita Emura (co-chair)	National Institute of Information and Communications Technology, Japan
Sebastian Faust	École Polytechnique Fédérale de Lausanne, Switzerland
Ryo Fujita	Chuo University, Japan
Goichiro Hanaoka (co-chair)	National Institute of Advanced Industrial Science and Technology, Japan
Noboru Kunihiro	The University of Tokyo, Japan
Benoît Libert	Technicolor, France
Shengli Liu	Shanghai Jiaotong University, China
Takahiro Matsuda	National Institute of Advanced Industrial Science and Technology, Japan
Jacob Schuldt	Royal Holloway, University of London, UK
Xun Yi	Victoria University, Australia
Kazuki Yoneyama	NTT, Japan
Jian Weng	Jinan University, China
Duncan S. Wong	City University of Hong Kong, Hong Kong
Fangguo Zhang	Sun Yat-sen University, China
Yunlei Zhao (co-chair)	Fudan University, China

(Last update: 2014 Feb 24)