The 5th ACM Asia Public Key Cryptography Workshop (APKC 2018)

Affiliated with ACM AsiaCCS 2018

June 4, 2018, Songdo, Incheon, Korea

Workshop website: https://www2.nict.go.jp/security/apkc2018/

Contact E-mail: apkc2018@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 1st edition of the event (ASIAPKC 2013) has been held in Hangzhou, China, the 2nd edition of the event (ASIAPKC 2014) has been held in Kyoto, Japan, the 3rd edition of the event (ASIAPKC 2016) has been held in Xi'an, China, and the 4th edition of the event (APKC 2017) has been held in Abu Dhabi, UAE. The 5th edition of the event (APKC 2018) will be held in Incheon, Korea, in conjunction with AsiaCCS 2018 (web: http://asiaccs2018.org/). As in the previous APKC series, the proceedings of APKC 2018 will be published by ACM Press and appear in ACM digital library.

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 for, and by, public-key cryptosystems
- 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
- Post-quantum public-key cryptography
- Fast implementation of public-key cryptosystems

We solicit systematization of knowledge (SoK) papers, which should aim to evaluate, systematize, and contextualize existing knowledge. Although Sok papers may not necessarily contain novel research contributions, such papers must provide a high value to our community. Submissions will be distinguished by the prefix "SoK:" in the title.

Important dates:

Submission due:	~~Jan 15, 2018~~ Jan 29, 2018 (Extended)
Notification:	Feb. 28, 2018
Proceedings version due:	Mar. 31, 2018
APKC workshop:	June 4, 2018

Submission website:

https://easychair.org/conferences/?conf=apkc2018

Instructions for authors: Technical papers submitted for APKC are to be written in English. Papers must be at most 8 pages excluding bibliography and appendices, and at most 10 pages in total. Committee members are not obligated to read appendices, and a paper must be intelligible without the appendices. Submissions must follow the new ACM conference template (https://www.acm.org/publications/proceedings-template), which has been updated for 2017 (Use sigconf style). Submissions should not use older ACM formats or non-standard formatting. Submissions must be in Portable Document Format (.pdf). Authors should devote special care that fonts, images, tables and figures comply with common standards and do not generate problems for reviewers.

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. Note that for attending APKC 2018, please make a registration for AsiaCCS 2018. 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 (NICT), Japan
Jae Hong Seo	Hanyang University, Korea
Yohei Watanabe	The University of Electro-Communications, Japan

Program Committee :

Nuttapong Attrapadung	AIST, Japan	Takahiro Matsuda	AIST, Japan
Joonsang Baek	University of Wollongong, Australia	Khoa Nguyen	Nanyang Technological University, Singapore
Jonathan Bootle	University College London, UK	Miyako Ohkubo	NICT, Japan
Jie Chen	East China Normal University, China	Ji Sun Shin	Sejong University, Korea
David Derler	Graz University of Technology, Austria	Daniel Slamanig	AIT Austrian Institute of Technology, Austria
Junqing Gong	ENS de Lyon, France	Atsushi Takayasu	The University of Tokyo, Japan
Jihye Kim	Kookmin University, Korea	Qiang Tang	New Jersey Institute of Technology, USA
Alexander Koch	KIT, Germany	Takashi Yamakawa	NTT Secure Platform Laboratories
Changmin Lee	Seoul National University, Korea	Kazuki Yoneyama	Ibaraki University, Japan
Hyung Tae Lee	Chonbuk National University, Korea	Rui Zhang	Chinese Academy of Sciences, China
Iraklis Leontiadis	EPFL, Switzerland		
Shengli Liu	Shanghai Jiao Tong University, China		

(Last update: 2018 March 1)