The 7th ACM Asia Public Key Cryptography Workshop (APKC 2020)

Affiliated with ACM AsiaCCS 2020 ~~June 1~~ October 6, 2020, Taipei, Taiwan

Workshop website: https://www2.nict.go.jp/security/apkc2020/

Contact E-mail: apkc2020@ml.nict.go.jp

Call for Papers

Due to the escalation of the COVID-19 situation around the world, AsiaCCS 2020 is rescheduled to October 5-9, 2020. APKC 2020 will be held on October 6.

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, the 4th edition of the event (APKC 2017) has been held in Abu Dhabi, UAE, the 5th edition of the event (APKC 2018) has been held in Incheon, Korea, and the 6th edition of the event (APKC 2019) has been held in Auckland, New Zealand. The 7th edition of the event (APKC 2020) will be held in Taipei, Taiwan in conjunction with AsiaCCS 2020 (https://asiaccs2020.cs.nthu.edu.tw/). As in the previous series, the proceedings of APKC 2020 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
- Public-key cryptography for cryptocurrencies
- Cryptographic protocols for blockchains
- Two-party and multi-party computations
- Card-based cryptographic protocols
- 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:	~~January 15, 2020~~ January 29, 2020 (Extended) (23:59, UTC)
Notification:	March 4, 2020
Proceedings version due:	March 30, 2020
APKC workshop:	~~June 1~~ October 6, 2020

Submission website:

https://easychair.org/conferences/?conf=apkc2020

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, which has been updated for 2019 (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.

APKC requires double-blind reviewing process. All submissions should be appropriately anonymized. Author names and affiliations should not appear in the paper. The authors should avoid obvious self-references and should appropriately blind them if used. The list of authors cannot be changed after the acceptance decision is made unless approved by the Program Chairs. Submissions to APKC 2020 must not substantially overlap with papers that are published or simultaneously submitted to other venues (including journals or conferences/workshops). Double-submission will result in immediate rejection. Detected violations may be reported to other conference chairs and journal editors. The Program Committee reserves the right to reject any paper that does not abide by the rules without considering its technical merits. Note that for attending APKC 2020, please make a registration for AsiaCCS 2020.

Program Co-Chairs:

Keita Emura	National Institute of Information and Communications Technology (NICT), Japan
Naoto Yanai	Osaka University, Japan

Program Committee:

Jonathan Bootle	IBM Research - Zurich, Switzerland	Khoa Nguyen	Nanyang Technological University, Singapore
Jie Chen	East China Normal University, China	Tran Viet Xuan Phuong	University of Wollongong, Australia
Long Chen	New Jersey Institute of Technology, USA	Yusuke Sakai	AIST, Japan
Kai-Min Chung	Academia Sinica, Taiwan	Jae Hong Seo	Hanyang University, Korea
Jason Paul Cruz	Osaka University, Japan	Daniel Slamanig	AIT Austrian Institute of Technology, Austria
Ruei-Hau Hsu	National Sun Yat-sen University, Taiwan	Atsushi Takayasu	National Institute of Information and Communications Technology (NICT), Japan
Alexander Koch	KIT, Germany	Raylin Tso	National Chengchi University, Taiwan
Pascal Lafourcade	Université Clermont Auvergne, LIMOS, France	Wen-Guey Tzeng	National Chiao Tung University, Taiwan
Hyung Tae Lee	Jeonbuk National University, Korea	Yohei Watanabe	The University of Electro-Communications, Japan
Iraklis Leontiadis	Inpher, Switzerland	Kazuki Yoneyama	Ibaraki University, Japan
Shengli Liu	Shanghai Jiao Tong University, China	Rui Zhang	Chinese Academy of Sciences, China

(Last update: 2020 April 1)