The 8th ACM Asia Public-Key Cryptography Workshop (APKC 2021)

Affiliated with ACM AsiaCCS 2021 June 7-11, 2021, Hong Kong, China

Workshop website: https://www2.nict.go.jp/security/apkc2021/

Contact E-mail: apkc2021@ml.nict.go.jp

Since ACM ASIACCS 2021 will be held as a virtual event due to COVID-19 from June 7th to June 11th, 2021, APKC 2021 also will be held as a virtual event.

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, 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, and the 7th edition of the event (APKC 2020) has been held in Taipei, Taiwan (Virtual Online). The 8th edition of the event (APKC 2021) will be held in Hong Kong, China, in conjunction with AsiaCCS 2021 (https://asiaccs2021.comp.polyu.edu.hk/). As in the previous series, the proceedings of APKC 2021 will be published by ACM Press and appear in ACM digital library. This workshop may grant the Best Paper Award. For the sake of fairness, we grant the award depending on aggregate score, and it should get no rejection from its every reviewer. If no such paper exists, workshop organizers will reserve the right to present the award.

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:	~~January8, 2021 (23:59 (UTC)~~ January 25, 2021 (23:59 (UTC) (Extended)
1st notification:	February 22, 2021
Resubmission due:	March 1, 2021
2nd notification:	March 8, 2021
Proceedings version due	March 31, 2021
APKC workshop:	June 7-11 (half-day event)

APKC 2021 adopts the following two-round submission policy. Basically, authors will receive either Accept or Reject in the 1st notification. Meanwhile, a few authors may receive a Resubmission Notification, which means that they are recommended to resubmit their papers with a reply letter. Then, they will receive either Accept or Reject in the 2nd notification. Note that this is NOT Conditional Acceptance, and the papers are automatically rejected if we did not get the authors' resubmission. We do not accept any new submission in the resubmission phase.

Submission website:

https://easychair.org/conferences/?conf=apkc2021

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 on September 21, 2020 (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 a 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 2021 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 2021, please make a registration for AsiaCCS 2021. For each workshopr paper requires a separate full pack or workshop only registration.

On conflicts of Interest; The program chairs require cooperation from both authors and program committee members to prevent submissions from being evaluated by reviewers who may have a conflict of interest. During the submission, authors should identify members of the program committee with whom they have a conflict of interest. Conflict of interest includes but not limited to: advisors and advisees (at any time in the past); authors and PC members who share an institutional relationship; professional collaborations (regardless of whether they resulted in a publication) that occurred in the past 2 years; line-of-management relationship, grant program manager, close personal relationships.

Program Co-Chairs:

Keita Emura	National Institute of Information and Communications Technology (NICT), Japan
Yuntao Wang	Japan Advanced Institute of Science and Technology (JAIST), Japan

Program Committee:

Jonathan Bootle	IBM Research - Zurich, Switzerland	Yuan Lu	Chinese Academy of Sciences, China
Xavier Bultel	INSA CVL, France	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	Jae Hong Seo	Hanyang University, Korea
K.P. Chow	The University of Hong Kong, China	Daniel Slamanig	AIT Austrian Institute of Technology, Austria
Shuichi Katsumata	National Institute of Advanced Industrial Science and Technology (AIST), Japan	Atsushi Takayasu	National Institute of Information and Communications Technology (NICT), Japan
Alexander Koch	Karlsruhe Institute of Technology (KIT), Germany	Yohei Watanabe	The University of Electro-Communications, Japan
Hyung Tae Lee	Jeonbuk National University, Korea	Naoto Yanai	Osaka University, Japan
Iraklis Leontiadis	Inpher, Switzerland	Kazuki Yoneyama	Ibaraki University, Japan
Shengli Liu	Shanghai Jiao Tong University, China	Rui Zhang	Chinese Academy of Sciences, China
Xingye Lu	The University of Hong Kong, China	Yongjun Zhao	Nanyang Technological University, Singapore

(Last update: 2021 January 25)