2022 IEEE THE 18TH ASIA PACIFIC CONFERENCE ON CIRCUITS AND SYSTEMS

APCCAS 2022 ASIA PACIFIC CONFERENCE ON CIRCUITS AND SYSTEMS

November 11-13, 2022 | Shenzhen, China

CONFERENCE INTRODUCTION

http://www.apccas2022.org/cfss.html

The IEEE Asia Pacific Conference on Circuits and Systems (APCCAS) is the regional flagship conference of the IEEE Circuits and Systems Society in Asia. APCCAS 2022 will be held in Shenzhen, China during November 11-13, 2022. Shenzhen is the electronics R&D world center with more than 300 global or regional centers from Fortune Global 500 companies. Besides, Shenzhen is also suitable for tourism, which is ranked No. 2 in the list of best cities for travel by Lonely Planet.

SPECIAL SESSION ON

Session Title	**Efficient Design for Post-Quantum Cryptography**
Special Session Organizer	**Jing Tian, Nanjing University** **Yuan Cao, Hohai University**

ABSTRACT

Due to recent progress in building quantum circuits, a large-scale quantum computer might become reality within the next 10 to 20 years. The hard mathematical problems (HMPs) underpinning the security of widely-used public-key cryptosystems like the Rivest-Shamir-Adleman (RSA) algorithm and elliptic-curve cryptography (ECC) could be easily solved by using Shor's algorithm on a large-scale quantum computer. Since 2017, the national institute of standards technology (NIST) has carried out three rounds of rigorous selection for the post-quantum cryptography (PQC) standardization progress. Currently, seven finalists and eight alternate candidates have been selected, whose HMPs mainly include lattice, code, multivariate, hash, and supersingular elliptic curve isogeny. Among them, the lattice based PQC (L-PQC) is the most popular, covering five finalists and two alternate candidates. This special session provides a forum to present and discuss high-efficiency designs for PQC, especially for L-PQC, where five talks are included. Three talks focus on solving the efficiency of the polynomial multiplication that is the major computation of L-PQC. One talk aims to improve the pseudo-random number generator. The last one is to discuss the effect of deep-learning based side channel analysis attack for the PQC designs.

IMPORTANT DATES

Submission of Special Session Full Papers	August 6, 2022

PUBLICATION

Accepted papers will be submitted for inclusion into IEEE Xplore subject to meeting IEEE Xplore's scope and quality requirements. Selected papers will be invited to submit extended full papers to IEEE Transaction on Circuits and Systems I (TCAS-I), IEEE Transaction on Circuits and Systems II (TCAS-II) and IEEE Open Journal of Circuits and Systems (OJCAS).

SUBMISSION METHOD

WORD

LATEX

Papers for publication must be submitted in full paper electronically. All edition and update must be done up until the submission deadline. Papers submitted to APCCAS Conference will undergo a double-blind review process. Submissions must have all details identifying the author(s) removed from the original manuscript (including authors' names, affiliations, acknowledgments and other related personal information).

Please make sure to use the standard IEEE conference templates to prepare your final manuscript, which can be found through link:

https://www.ieee.org/content/dam/ieee-org/ieee/web/org/conferences/conference-template-a4.docx

SUBMISSION LINK

http://www.easychair.org/conferences/?conf=apccas2022

Sponsored by

IEEE CAS IEEE CIRCUITS AND SYSTEMS SOCIETY

Hosted by

Co-sponsored by

CAS IEEE CIRCUITS AND SYSTEMS SOCIETY Shenzhen Chapter

深圳大学 SHENZHEN UNIVERSITY

清华大学深圳国际研究生院 Tsinghua Shenzhen International Graduate School

北京大学深圳研究生院 Peking University Shenzhen Graduate School

CONTACT Tel.: +86-28-87555888 Mob.: +86-13688349945 Email: info@apccas2022.org