IEEE Design&Test

Call for Papers for a Special Issue on
Post-Quantum Cryptography for Internet-of-Things (IoT)

Aim and Scope

A time frame of 10-15 years is predicted by many researchers for the wide-spread deployment of quantum computers. They are poised to break all mainstream public-key cryptographic schemes, which are currently used in many industrial control networks, public key infrastructures (PKI), and blockchain-based technologies. In 2014, the National Institute of Standards and Technology (NIST) suggested that a quantum computer capable of breaking RSA could be built by 2030. The National Security Agency (NSA) warned in 2015 that progress in quantum computing has reached a point that organizations should start deploying encryption algorithms designed to withstand attacks performed on quantum computers. Since 2020, there has been a final recommendation from NIST for stateful hash-based signatures and a total of 7 finalists for public-key encryption, key encapsulation mechanisms, and digital signatures. Two key aspects to enable a smooth transition from current cryptographic algorithms, such as RSA and ECC, to post-quantum algorithms are implementation security and performance. This is especially true for constrained devices such as IoT platforms in several application domains such as industrial networks, smart and critical infrastructures, banking, e-health, and transportation. This transition, generally termed as *Crypto Agility,* underscores an urgent need for evaluating post-quantum cryptographic implementations on IoT platforms for physical security and performance, including the integration of such implementations in current protocols and systems.

Topics of Interest

This special issue is dedicated to post-quantum cryptography for IoT platforms. It aims to cover diverse aspects of theory and implementation of post-quantum cryptographic algorithms, their security analysis, and benchmarking. The specific topics of interest include but are not limited to:

- Efficient (Runtime, Energy, Area) implementations of PQC primitives on microcontrollers, FPGAs, ASICs with specific focus on IoT platforms
- Studies on side-channel attacks of post-quantum cryptographic implementations on IoT platforms
- Robust PQC implementations with proven countermeasures against physical attacks
- Performance benchmarking of post-quantum cryptographic implementations in standard protocols
- Migration strategies and configurable implementations of PQC using IoT platforms in current protocols and systems
- Design, analysis and implementations of Hardware Security Modules (HSMs) based on PQC algorithms

Submission Guidelines

Prospective authors should follow the submission guidelines for IEEE Design & Test. All manuscripts must be submitted electronically to IEEE Manuscript Central at https://mc.manuscriptcentral.com/dandt. Indicate that you are submitting your article to the "*Special Issue on Post-Quantum Cryptography for Internet-of-Things (IoT)*". Manuscripts must not exceed 5,000 words, including figures (with each average-size figure counting as 200 words) and a maximum of 12 references (30 for surveys). This amounts to about 4,000 words of text and a maximum of five small to medium figures. Accepted articles will be edited for clarity, structure, conciseness, grammar, passive to active voice, logical organization, readability, and adherence to style. Please see IEEE Design & Test Author Information at: https://ieee-ceda.org/publication/ieee-design-test-dt/author-info.

Schedule

- Open for submissions : September 1, 2022
- Submission deadline : November 1, 2022
- Notification First Round : January 15, 2023
- Revision submission : March 31, 2023
- Final decisions : May 15, 2023
- Tentative publication : Fall 2023

Guest Editors

- **Shivam Bhasin**, Nanyang Technological University, Singapore
- **Anupam Chattopadhyay**, Nanyang Technological University, Singapore
- **Tim Güneysu**, Ruhr University Bochum, Germany
- **Swarup Bhunia**, University of Florida, USA

For questions and further information, please contact the lead guest editor at: anupam@ntu.edu.sg