IEEE JOURNAL ON
EMERGING AND SELECTED TOPICS IN CIRCUITS AND SYSTEMS

CALL for PAPERS

Efficient and Secure Hardware Acceleration for Post-Quantum Cryptography

Guest editors

- Jiafeng Xie, Villanova University, USA (jiafeng.xie@villanova.edu)
- Dur-E-Shahwar Kundi, PQShield Ltd., UK (dur-e-shahwar.kundi@pqshield.com)
- Yuichi Hayashi, Nara Institute of Science and Technology, Japan (yu-ichi@is.naist.jp)
- Máire O'Neill, Queen's University Belfast, UK (m.oneill@ecit.qub.ac.uk)

Scope and purpose

The rapid progress in quantum computing has initiated a new wave of cryptosystem innovation, i.e., quantum-resistant cryptography, also widely referred to as post-quantum cryptography (PQC). PQC is a new type of cryptosystem that can resist quantum attacks, and has recently attracted significant attention from the research community. In particular, the United States National Institute of Standards and Technology (NIST) has initiated a PQC standardization process, and so far, five algorithms have been selected for standardization. Besides that, an additional round of digital signature scheme standardization is on-going, where several other types of PQC algorithms are being considered currently. Alongside these standardization efforts, research is increasingly shifting towards hardware acceleration (one main reason is that hardware acceleration typically offers better performance compared to software). However, hardware-accelerated PQC designs, on platforms like FPGAs (field-programmable gate array) and ASICs (application-specific integrated circuit), face significant security issues before actual deployment, e.g., vulnerability to side-channel analysis and other attacks.

Since the selected PQC schemes (including those under consideration) are based on different types of cryptographic hard problems and possess unique features, achieving efficient and secure hardware acceleration of these PQC is both highly challenging and of great interest: (i) PQC standardization has entered a phase where implementation security demands greater attention. However, research into the security of hardware-accelerated PQC designs, such as against side-channel attacks, remains underexplored. (ii) Further research is also needed into new attack mitigation strategies for hardware PQC designs that are secure yet efficient. (iii) The new hardware acceleration and related security analysis for PQC algorithms have not been adequately explored.

This special issue aims to deliver comprehensive and multidisciplinary research into efficient and secure hardware acceleration for PQC. The targeted research topics will cover different hardware acceleration methods, benchmarking methodologies, major component and arithmetic techniques, cross-layer side-channel leakage assessment, system integration, lightweight design, architectural innovations for secure design, reliability, automation design tools, emerging acceleration techniques and security analysis, etc. We hope this special issue will stimulate further research in the field, provide insightful information to the community, and inspire follow-up work in this important area.

Topics of interest

Topics of interest to this special issue include contributions related to securing hardware acceleration for PQC. More specifically, these may include, but not limited to, the following:

- Efficient hardware acceleration for different types of PQC algorithms, including lattice-based, hash-based, code-based, etc.
- New hardware-software co-design for PQC, acceleration of PQC on other hardware platforms like GPU, and related security analysis
- New benchmarking methodologies and performance optimization for efficient and secure hardware acceleration of PQC with respect to different implementation platforms
- New hardware acceleration for PQC core arithmetic and computation-intensive operations
- Novel arithmetic techniques for side-channel countermeasure development
- Exploration of cross-layer security vulnerabilities in hardware-designed PQC accelerators, with respect to different applications (from major components to system-level operations)
- System integration and deployment of securely implemented PQC hardware accelerators
- Novel lightweight acceleration for PQC, including side-channel analysis and lightweight countermeasure designs
- Architectural innovations aimed at secure acceleration for PQC, including (not limited to) standalone, reconfigurable, ASIC-based, FPGA-based, and instruction-set architectures
- Reliability and robustness for PQC hardware accelerators, e.g., error resilience, fault tolerance
- Design automation and tools for efficient and secure hardware acceleration of PQC, e.g., new pre-silicon simulation for side-channel leakage assessment and countermeasure design
- Emerging hardware acceleration and security analysis for PQC, e.g., AI-assisted design

Submission procedure

Prospective authors are invited to submit their papers following the instructions provided on the IEEE JETCAS website: https://ieee-cas.org/publication/JETCAS/manuscript-submission-guide. The submitted manuscripts should not have been previously published, nor should they be currently under consideration for publication elsewhere. The IEEE JETCAS submission site: https://ieee.atyponrex.com/journal/jetcas

Important dates

- **Manuscript submissions due: September 1, 2026**
- **First round of reviews completed: November 17, 2026**
- **Revised manuscripts due: December 8, 2026**
- **Second round of reviews completed: January 1, 2027**
- **Final manuscripts due: January 15, 2027**

Request for information

Corresponding Guest Editor (CGE): Jiafeng Xie (jiafeng.xie@villanova.edu)