Special Issue

Side-Channel and Fault Attacks in Post-quantum Cryptography

Message from the Guest Editors

Post-quantum cryptography (PQC) is a research subject investigating public-key cryptographic algorithms that are believed to resist quantum attacks. On July 5, 2022, NIST announced the selected KEM and digital signature candidates to be standardized in their PQC standardization project. The need to securely implement PQC schemes will drastically increase in the coming years as many commercial products or open-source hardware/software have planned the transition to PQC solutions. In this Special Issue, we are particularly interested in discovering new side-channel and fault attacks against known PQC implementations and proposing more efficient and secure countermeasures. Topics of interest include but are not limited to:

- Power and EM side-channel attacks on post-quantum implementations
- Micro-architectural side-channel attacks on post-quantum implementations
- Masked implementations in post-quantum cryptography
- Efficient constant-time post-quantum implementations
- Fault attacks and countermeasures in post-quantum cryptography
- Attacks and countermeasures on Fully Homomorphic Encryption (FHE) implementations

Guest Editors

Dr. Qian Guo

Department of Electrical and Information Technology, Lund University, 221 00 Lund, Sweden

Dr. Ali Hassan Sodhro

Department of Computer Science, Kristianstad University, SE-291 88 Kristianstad, Sweden

Deadline for manuscript submissions

closed (20 October 2024)

Electronics

an Open Access Journal by MDPI

Impact Factor 2.6
CiteScore 6.1

mdpi.com/si/135919

Electronics
Editorial Office
MDPI, Grosspeteranlage 5
4052 Basel, Switzerland
Tel: +41 61 683 77 34
electronics@mdpi.com

mdpi.com/journal/electronics

Electronics

an Open Access Journal by MDPI

Impact Factor 2.6
CiteScore 6.1

mdpi.com/journal/electronics

About the Journal

Message from the Editor-in-Chief

Electronics is a multidisciplinary journal designed to appeal to a diverse audience of research scientists, practitioners, and developers in academia and industry. The journal is devoted to fast publication of latest technological breakthroughs, cutting-edge developments, and timely reviews of current and emerging technologies related to the broad field of electronics. Experimental and theoretical results are published as regular peer-reviewed articles or as articles within Special Issues guestedited by leading experts in selected topics of interest.

Editor-in-Chief

Prof. Dr. Flavio Canavero
Department of Electronics and Telecommunications, Politecnico di Torino, 10129 Torino, Italy

Author Benefits

High Visibility:

indexed within Scopus, SCIE (Web of Science), CAPlus / SciFinder, Inspec, Ei Compendex and other databases.

Journal Rank:

JCR - Q2 (Engineering, Electrical and Electronic) / CiteScore - Q1 (Electrical and Electronic Engineering)

Rapid Publication:

manuscripts are peer-reviewed and a first decision is provided to authors approximately 16.8 days after submission; acceptance to publication is undertaken in 2.4 days (median values for papers published in this journal in the first half of 2025).

MDPI