electronics

an Open Access Journal by MDPI

IMPACT FACTOR 2.6

CITESCORE 5.3

Side-Channel and Fault Attacks in Post-quantum Cryptography

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-29188 Kristianstad, Sweden

Deadline for manuscript submissions:
20 October 2024

Message from the Guest Editors

Dear Colleagues,

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

electronics

IMPACT FACTOR 2.6

CITESCORE 5.3

an Open Access Journal by MDPI

Editor-in-Chief

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

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 guest-edited by leading experts in selected topics of interest.

Author Benefits

Open Access: free for readers, with article processing charges (APC) paid by authors or their institutions.
High Visibility: indexed within Scopus, SCIE (Web of Science), CAPlus / SciFinder, Inspec, Ei Compendex and other databases.
Journal Rank: JCR - Q2 (*Physics, Applied*) / CiteScore - Q2 (*Control and Systems Engineering*)

Contact Us

Electronics Editorial Office
MDPI, Grosspeteranlage 5
4052 Basel, Switzerland

Tel: +41 61 683 77 34
www.mdpi.com

mdpi.com/journal/electronics
electronics@mdpi.com
𝕏@electronicsMDPI