Special Issue

Advances in Post-Quantum Cryptography

Message from the Guest Editors

Quantum computation is currently one the most biggest threat to cryptography. Theoretically, the security of modern cryptography is built on computational complexity theory, while quantum computation has changed the edge and structure of the computational complexity map and thus brings a transformative threat to the cryptography field. To prepare for the threat of quantum computing, many countries and international standard organizations have initiated the standardization and migration of post-quantum cryptography. To promote the development of post-quantum cryptography, we are organizing this Special Issue. Topics of interest include, but not limited to, the foundational theory of quantum secure cryptography; design and analysis of post-quantum cryptography schemes; implementation of post-quantum cryptography based on CPU, FPGA, GPU, ASIC, ARM, and RISC-V; security proof in the quantum random oracle model; design and analysis of quantum circuit for cryptography; migration of secure protocols; and applications of post-quantum cryptography in financial systems, mobile communication, power systems, intelligent transportation systems, and blockchain.

Guest Editors

Dr. Xianhui Lu

Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China

Prof. Dr. Jianfeng Wang

School of Cyber Engineering, Xidian University, Xi'an 710126, China

Deadline for manuscript submissions

20 December 2026

Cryptography

an Open Access Journal by MDPI

Impact Factor 2.4
CiteScore 6.4

mdpi.com/si/257582

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

mdpi.com/journal/cryptography

Cryptography

an Open Access Journal by MDPI

Impact Factor 2.4
CiteScore 6.4

mdpi.com/journal/cryptography

About the Journal

Message from the Editor-in-Chief

Cryptography is a new international journal which provides the state-of-the-art forum for original results in all areas of modern cryptography. *Cryptography* is published in open access format: research articles, reviews and other contents are released on the internet immediately after acceptance. Our journal welcomes submissions written from the theory and practices of modern cryptography, so that it may become a forum for exchange of new scientific developments between the cryptographers and the practitioners.
We would be pleased to welcome you as one of our authors.

Editor-in-Chief

Prof. Dr. Josef Pieprzyk
1. Data61, CSIRO (the Commonwealth Scientific and Industrial Research Organisation), Sydney, NSW 2000, Australia
2. Institute of Computer Science, Polish Academy of Science, 02-668 Warszawa, Poland

Author Benefits

Open Access:

free for readers, with article processing charges (APC) paid by authors or their institutions.

High Visibility:

indexed within Scopus, ESCI (Web of Science), dblp, and other databases.

Journal Rank:

JCR - Q2 (Computer Science, Theory and Methods) / CiteScore - Q1 (Applied Mathematics)

MDPI