Special Issue

Recent Advances in Post-Quantum Cryptography

Message from the Guest Editors

In response to the rapid development of quantum computing, post-quantum cryptography (PQC) has made significant strides, aiming to develop algorithms that are both secure against quantum adversaries and efficient for practical use. The 2024 NIST announcement of the Kyber (KEM), Dilithium, and SPHINCS+ (digital signatures) standards marks a critical milestone in PQC. Complementing these standards, frameworks like NIST's SP 800-227 are being developed to guide the secure implementation and use of these algorithms, further bridging the gap between theory and real-world application. This Special Issue invites contributions focused on recent advances in PQC. Topics of interest include, but are not limited to, the following:

- Designs and implementation in migration to PQC;
- Security analysis and attack mitigation strategies;
- Efficient implementations and performance optimization;
- Integration of PQC into existing protocols and systems;
- Side-channel attacks and countermeasures in PQC;
- Quantum-resistant blockchain and IoT technologies;
- Practical challenges in transitioning to post-quantum standards.

Guest Editors

Dr. Chi Cheng

Prof. Dr. Jintai Ding

Dr. Yanbin Pan

Deadline for manuscript submissions

31 August 2025

Mathematics

an Open Access Journal by MDPI

Impact Factor 2.2
CiteScore 4.6

mdpi.com/si/230465

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

mdpi.com/journal/mathematics

MDPI

Σ

Mathematics

an Open Access Journal
by MDPI

Impact Factor 2.2
CiteScore 4.6

mdpi.com/journal/
mathematics

MDPI

About the Journal

Message from the Editor-in-Chief

The journal *Mathematics* publishes high-quality, refereed papers that treat both pure and applied mathematics. The journal highlights articles devoted to the mathematical treatment of questions arising in physics, chemistry, biology, statistics, finance, computer science, engineering and sociology, particularly those that stress analytical/algebraic aspects and novel problems and their solutions. One of the missions of the journal is to serve mathematicians and scientists through the prompt publication of significant advances in any branch of science and technology, and to provide a forum for the discussion of new scientific developments.

Editor-in-Chief

Prof. Dr. Francisco Chiclana
School of Computer Science and Informatics, De Montfort University,
The Gateway, Leicester LE1 9BH, UK

Author Benefits

High Visibility:

indexed within Scopus, SCIE (Web of Science), RePEc, and other databases.

Journal Rank:

JCR - Q1 (Mathematics) / CiteScore - Q1 (General Mathematics)

Rapid Publication:

manuscripts are peer-reviewed and a first decision is provided to authors approximately 18.4 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).