cryptography

IMPACT FACTOR 1.8

CITESCORE 3.8

an Open Access Journal by MDPI

Public-Key Cryptography in the Post-quantum Era

Guest Editors:

Dr. Edoardo Persichetti

Dr. Paolo Santini

Dr. Marco Baldi

Prof. Dr. Qiang Wang

Deadline for manuscript submissions:
closed (31 December 2021)

Message from the Guest Editors

Public-key cryptography is one of the fundamental tools to achieve secure communications in the modern world. The security of traditional public-key primitives, however, is threatened by Shor's algorithm. This has prompted institutes such as NIST to prepare the ground for post-quantum standardization. Consequently, the field has seen a surge in research activity and quickly risen to a prominent position in the current cryptographic domain.

Lattice-based cryptography is the largest and most promising research area in the context of post-quantum cryptography. Code-based cryptosystems are also very popular.

In this Special Issue, we aim to collect contributions which are broadly related to post-quantum cryptography, including (but not limited to):

- Design of post-quantum cryptographic primitives;
- Code-based cryptography;
- Lattice-based cryptography;
- Multivariate cryptography;
- Isogeny-based cryptography;
- Cryptanalysis of post-quantum cryptosystems;
- Provable security in the ROM and QROM;
- Software and hardware implementations;
- Performance and security analysis of NIST candidates.

mdpi.com/si/70575