# **Special Issue**

# Public-Key Cryptography in the Post-quantum Era

## 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.

### Guest Editors

Dr. Edoardo Persichetti

Dr. Paolo Santini

Dr. Marco Baldi

Prof. Dr. Qiang Wang

### Deadline for manuscript submissions

closed (31 December 2021)



# Cryptography

an Open Access Journal by MDPI

Impact Factor 1.8 CiteScore 3.8



mdpi.com/si/70575

*Cryptography* 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 1.8 CiteScore 3.8



cryptography



# About the Journal

### Message from the Editor-in-Chief

#### Editor-in-Chief

#### Prof. Dr. Josef Pieprzyk

1. Data61, CSIRO (The Commonwealth Scientific and Industrial Research Organisation), Sydney, NSW 2000, Australia 2. Insitute 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)

