mathematics

an Open Access Journal by MDPI

IMPACT FACTOR 2.3

CITESCORE 4.0

Post-quantum Lightweight Cryptography

Guest Editor:

Prof. Dr. Danilo Gligoroski
Department of Information Security and Communication Technology, Norwegian University of Science and Technology, 7491 Trondheim, Norway

Deadline for manuscript submissions:
closed (31 March 2021)

Message from the Guest Editor

Dear Colleagues,

There is a strong need for reliable post-quantum lightweight cryptography.

We are on the brink of the next major shift in the ICT revolution, with the advent of the Internet of Things (IoT) and fifth generation (5G) mobile communications. Currently, there are around 21 billion connected IoT devices, and it is projected that there will be more than 75 billion IoT devices worldwide by 2025. One indisputable fact is that most of these newly networked devices have limited resources. The current standards for symmetric cryptography have been optimized for desktop and server environments. When it comes to resource-constrained devices, these primitive standards are very difficult or impossible to implement. These issues are the subject of the current NIST Lightweight Cryptography Standardization project, which is seeking lightweight authenticated encryption and lightweight hash functions .

The situation for post-quantum public-key schemes that can be implemented and used in resource-constrained devices is even more dramatic. The reasons for this are that post-quantum designs have significantly larger public keys, larger signatures, or larger ciphertexts.

mathematics

IMPACT FACTOR 2.3

CITESCORE 4.0

an Open Access Journal by MDPI

Editor-in-Chief

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

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.

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), RePEc, and other databases.
Journal Rank: JCR - Q1 (Mathematics) / CiteScore - Q1 (General Mathematics)

Contact Us

Mathematics Editorial Office
MDPI, Grosspeteranlage 5
4052 Basel, Switzerland

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

mdpi.com/journal/mathematics
mathematics@mdpi.com
𝕏@MathematicsMDPI