



## Design and Analysis of Symmetric Encryption Modes of Operation

Guest Editors:

**Dr. Fajiang Yu**

School of Computer, Wuhan  
University, Wuhan 430072, China

**Prof. Dr. Kuo-Hui Yeh**

Institute of Artificial Intelligence  
Innovation, National Yang Ming  
Chiao Tung University, Hsinchu  
300093, Taiwan

**Dr. Zhangyi Wang**

School of Computer, Wuhan  
University, Wuhan 430072, China

Deadline for manuscript  
submissions:

**31 August 2024**

### Message from the Guest Editors

A symmetric encryption mode of operation refers to the method used to transform data larger than a single block using a cipher's single-block operation. The mode of operation plays a crucial role in providing information confidentiality, authenticity, and integrity. This Special Issue of *Symmetry* aims to cover various topics related to symmetric encryption modes of operation. These may include, but are not limited to:

1. Security evaluation and attacks on operation modes and their variants;
2. Application of operation modes or the design of new modes for constructing pseudorandom number generators, hash functions, message authentication codes, cryptographic protocols, and more;
3. Application of operation modes or the design of new modes for data encryption in database buffer pools, cloud data encryption, parallel encryption, data security and privacy protection in federated learning, and other related areas;
4. Analysis of the misuses of operation modes in security schemes or implementations.





an Open Access Journal by MDPI

## Editor-in-Chief

### Prof. Dr. Sergei D. Odintsov

1. Institució Catalana de Recerca  
i Estudis Avançats (ICREA),  
Passeig Luis Companys, 23,  
08010 Barcelona, Spain  
2. Institute of Space Sciences  
(ICE-CSIC), C. Can Magrans s/n,  
08193 Barcelona, Spain

## Message from the Editor-in-Chief

Symmetry is ultimately the most important concept in natural sciences. It is not surprising then that very basic and fundamental research achievements are related to symmetry. For instance, the Nobel Prize in Physics 1979 (Glashow, Salam, Weinberg) was received for a unified symmetry description of electromagnetic and weak interactions, while the Nobel Prize in Physics 2008 (Nambu, Kobayashi, Maskawa) was received for the discovery of the mechanism of spontaneous breaking of symmetry, including CP symmetry. Our journal is named *Symmetry* and it manifests its fundamental role in nature.

## 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), CAPlus / SciFinder, Inspec, Astrophysics Data System, and other databases.

**Journal Rank:** JCR - Q2 (*Multidisciplinary Sciences*) / CiteScore - Q1 (*General Mathematics*); Q1 (*Physics and Astronomy*); Q1 (*Computer Science*)

## Contact Us

Symmetry Editorial Office  
MDPI, St. Alban-Anlage 66  
4052 Basel, Switzerland

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

mdpi.com/journal/symmetry  
symmetry@mdpi.com  
X@Symmetry\_MDPI