

# Special Issue

## Side Channel and Fault Injection Attacks and Countermeasures

### Message from the Guest Editors

With the current massive growth of embedded devices dealing with sensitive information from different fields (e.g. automotive, banking, medical, electronic-ID) and with the exponential increase in the number of connected devices from the Internet of Things, physical security has taken a central position in research.

This special issue focuses on the general topic of physical security in theory and in practice, from the design of state-of-the-art attacks, countermeasures, provable secure implementations and security evaluations. Areas of interest include:

- Symmetric/asymmetric cryptography
- Side-channel attacks
- Fault attacks
- Probing model and masking schemes
- Software/Hardware countermeasures
- Secure implementations
- Security evaluation

---

### Guest Editors

Prof. Dr. Claude Carlet

Dr. Pierrick Méaux

Dr. Romain Poussier

---

### Deadline for manuscript submissions

closed (30 October 2020)



## Cryptography

---

an Open Access Journal  
by MDPI

---

Impact Factor 2.1  
CiteScore 5.0



[mdpi.com/si/38646](https://mdpi.com/si/38646)

*Cryptography*  
Editorial Office  
MDPI, Grosspeteranlage 5  
4052 Basel, Switzerland  
Tel: +41 61 683 77 34  
[cryptography@mdpi.com](mailto:cryptography@mdpi.com)

[mdpi.com/journal/  
cryptography](https://mdpi.com/journal/cryptography)





# Cryptography

---

an Open Access Journal  
by MDPI

---

Impact Factor 2.1  
CiteScore 5.0



[mdpi.com/journal/  
cryptography](https://mdpi.com/journal/cryptography)



## About the Journal

### Message from the Editor-in-Chief

*Cryptography* is a new international journal which provides the state-of-the-art forum for original results in all areas of modern cryptography. *Cryptography* is published in open access format: research articles, reviews and other contents are released on the internet immediately after acceptance. Our journal welcomes submissions written from the theory and practices of modern cryptography, so that it may become a forum for exchange of new scientific developments between the cryptographers and the practitioners.

We would be pleased to welcome you as one of our authors.

---

### Editor-in-Chief

Prof. Dr. Josef Pieprzyk

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

2. Institute 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)