Special Issue

Fault Analysis in Cryptography

Message from the Guest Editors

The pervasiveness of embedded devices in our everyday world is apparent. With paradigms such as Internet-of-Things, Edge Computing, Industry 4.0, the importance of small computing devices is higher than ever. However, as these devices are often placed in uncontrolled, potentially hostile environments, security evaluations need to consider physical security threats. Fault injection attacks fall within this category, being a well-researched area that focuses on breaking cryptographic implementations by actively tampering with the device. For over two decades, researchers have been developing novel fault analysis methods, fault injection techniques, and countermeasures. The focus of this Special Issue covers all aspects of fault analysis in cryptography. This includes, but is not limited to, novel attacks and protections on both symmetric and public key cryptography, experimental evaluations, automated techniques, security proofs, and standardization methods.

Guest Editors

Dr. Jakub Breier
Silicon Austria Labs, 8010 Graz, Austria
Dr. Xiaolu Hou
Faculty of Informatics and Information Technologies, Slovak University of Technology, 811 07 Bratislava, Slovakia

Deadline for manuscript submissions

closed (15 February 2022)

Cryptography

an Open Access Journal by MDPI

Impact Factor 2.1
CiteScore 5.0

mdpi.com/si/84495

Cryptography
Editorial Office
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 2.1
CiteScore 5.0

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)

MDPI