Special Issue

Implementation and Verification of Secure Hardware against Physical Attacks

Message from the Guest Editors

Secured electronic systems are of paramount importance for all computational platforms and for various applications. Implementation-related aspects of cryptographic systems and their real-world sensitivities is in the focus of this Special Issue Guidelines: Authors are invited to submit a title and an extended abstract of the proposed manuscript, potentially covering, but not limited to, the following topics:

- Hardware security analysis of primitives
- Protection mechanisms for symmetric/asymmetric designs (e.g., facing horizontal attacks)
- Side-channel analysis, including attack modeling, simulation and countermeasures.
- Fault injection, detection, attacks and modeling
- Analysis, modeling and implementation aspects of true random number generators (TRNGs) and physically unclonable functions (PUFs)
- Protection from AI architectures and AI-assisted attacks supported by rigorous analysis
- Analysis of hardware trojans and devices' reconfigurability/reprogramming
- Validation and evaluation methodologies for physical security
- Novel and emerging technologies for security application

Guest Editors

Dr. Itamar Levi

Dr. Johann Knechtel

Prof. Dr. Selçuk Köse

Dr. Giuseppe Scotti

Deadline for manuscript submissions

closed (15 March 2022)

Cryptography

an Open Access Journal by MDPI

Impact Factor 2.1
CiteScore 5.0

mdpi.com/si/77005

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