cryptography

an Open Access Journal by MDPI

IMPACT FACTOR 1.8

CITESCORE 3.8

Implementation and Verification of Secure Hardware against Physical Attacks

Guest Editors:

Dr. Itamar Levi

Dr. Johann Knechtel

Prof. Dr. Selçuk Köse

Dr. Giuseppe Scotti

Deadline for manuscript submissions:
closed (15 March 2022)

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

mdpi.com/si/77005

Special Issue