cryptography

an Open Access Journal by MDPI

IMPACT FACTOR 1.8

CITESCORE 3.8

Fault Analysis in Cryptography

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)

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.