cryptography

an Open Access Journal by MDPI

IMPACT FACTOR 1.6

CITESCORE 3.6

Side Channel and Fault Injection Attacks and Countermeasures

Guest Editors:

Prof. Dr. Claude Carlet
Department of Informatics, University of Bergen, N-5008 Bergen, Norway; Département de mathématiques, Université Paris 8, 93526 Saint-Denis, France

Dr. Pierrick Méaux
Institue of Information and Communication Technologies, Electronics and Applied Mathematics, Université catholique de Louvain, 1348 Ottignies-Louvain-la-Neuve, Belgium

Dr. Romain Poussier
Nanyang Technological University, Temasek Laboratories, 50 Nanyang Drive, Research Techno Plaza, BorderX Block, 9th Storey, Singapour 637553, Singapore

Deadline for manuscript submissions:
closed (30 October 2020)

Message from the Guest Editors

Dear Colleagues,

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

mdpi.com/si/38646

Special Issue