Special Issue

Physical Layer Security and Trust for Legacy Systems and Supply Chain Assurance

Message from the Guest Editor

Physical-layer security and trust of microelectronic systems is threatened by side-channel signal acquisition attacks, semi-invasive probing and sophisticated reverse engineering process flows. Legacy systems are particularly vulnerable and the large investment in current deployments across medical, military, industrial, and critical infrastructures makes it imperative that these systems are retrofit with countermeasures designed to improve their situational-awareness and resilience to attacks. Techniques that provide a root-of-trust through, for example, secure boot, and/or provide intra-SoC security firewalls between IP blocks would further improve the resilience of both legacy and emerging systems. Similarly, methods that provide assurance of authenticity of chips and systems as they move through the supply chain would also greatly alleviate security concerns related to hidden back door access mechanisms in newly deployed systems. This Special Issue covers these topics as well as extended versions of papers presented at the HOST 2018 (http://www.hostsymposium.org/).

Guest Editor

Prof. Dr. Jim Plusquellic

Department of Electrical and Computer Engineering, University of New Mexico, Albuquerque, NM 87131, USA

Deadline for manuscript submissions

closed (31 July 2018)

Cryptography

an Open Access Journal by MDPI

Impact Factor 2.1
CiteScore 5.0

mdpi.com/si/15222

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

MDPI

About the Journal

Message from the Editor-in-Chief

Editor-in-Chief

Prof. Dr. Josef Pieprzyk
1. Data61, CSIRO (The Commonwealth Scientific and Industrial Research Organisation), Sydney, NSW 2000, Australia
2. Insitute 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)