cryptography

an Open Access Journal by MDPI

IMPACT FACTOR 1.8

CITESCORE 3.8

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

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)

Message from the Guest Editor

Dear Colleagues,

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/).

Prof. Dr. Jim Plusquellic
Guest Editor