IEEE Internet of Things Journal
Call for Papers - Special Issue on:

Intrinsic Hardware Security for Internet of Things Infrastructure

Internet of Things (IoT) is an emerging technology in the modern era of big data. It concerns a variety of applications ranging from smart homes, connected vehicles to smart factories and more. IoT infrastructure typically comprises millions of connected objects and devices that store and exchange sensitive and confidential information. Theft and fraud scenarios, such as hacking and identity forgery, are serious threats to such IoT devices. Embedded hardware security techniques could be a potential solution to preserve the highest level of security within this infrastructure.

Physically unclonable functions (PUFs) are among the potential solution to data security and counterfeiting problems. On-chip security can be implemented during chip production utilizing chip integration techniques. Recently, nanostructured PUF security have been proposed as a promising intrinsic security solution as well. Many more intrinsic hardware security techniques are underway for a highly-secure IoT infrastructure as strongly demanded by the IoT community.

The focus of this special issue is to provide readers with the latest advances in securing IoT infrastructure from the physical layer point-of-view. IEEE Journal of Internet of Things invites authors to submit original contributions and survey manuscripts to this special issue. Some of the topics to be covered here include (but are not limited to):

- Physically Unclonable Functions (PUFs).
- Nanostructured PUFs.
- Inkjet-Printed PUFs.
- RF Fingerprinting Techniques.
- Embedded Chip Security.
- Secure Near-Field Communications.
- Applied Cryptographic Algorithms.
- Optical PUFs.
- Securing RFID Grids.
- Hardware-Based Cryptography.
- Novel Intrinsic Security Issues.
- RF Certificates-of-Authenticity (RFCoA).
- RF Distinct Native Attributes (RF-DNA).
- PUF Integration and Packaging.
- Fingerprint Classification Techniques.
- Hardware Level Security for LPWANs.
- Secret Key Generation.
- Hardware-based Security Protocols.
- Physically Obfuscated Keys (POKs).
- Integrated RFID Security.

Important Dates:

Submissions Deadline: **February 15, 2018** First Reviews Due: **May 1, 2018** Revision Due: **June 1, 2018**	Second Reviews Due/Notification: **July 1, 2018** Final Manuscript Due: **August 1, 2018** Publication Date: **2018**

Submission:

All original manuscripts or revisions to the IEEE IoT Journal must be submitted online through IEEE Manuscript Central http://mc.manuscriptcentral.com/iot.

Author guidelines and submission information can be found at http://ieee-iotj.org

Guest Editors:

Dr. Mohamed Kheir (Lead Guest Editor)
IMS Connector Systems GmbH, Germany
mohamed.kheir@ieee.org

Prof. Manos Tentzeris
Georgia Institute of Technology, USA
etentze@ece.gatech.edu

Prof. Ahmed Abdelgawad
Central Michigan University, USA
abdel1a@cmich.edu,

Prof. Ilsun You
Soonchunhyang University, South Korea
ilsunu@gmail.com

Dr. Darko Kirovski
Jump Trading LLC., USA
darko@kirovski.org