Guest Editors' Introduction

Physical Unclonable Function (PUF) based Sustainable Cybersecurity

Himanshu Thapliyal
University of Kentucky

Saraju P. Mohanty
University of North Texas

This special section investigates the potential use of Physically Unclonable Functions (PUFs) as a hardware security approach for sustainable cybersecurity. PUFs are a class of circuits that use the inherent variations in the Integrated Circuit manufacturing process to create unique and unclonable IDs [1]. PUF has the potential to seal multiple types of vulnerabilities for sustainable cybersecurity specifically in the security classes of authentication, non-repudiation, and privacy. PUF designs are proposed using a variety of techniques and implementation mediums (see Figure 1) [1]. The common ground between the designs is leveraging intrinsic variations that should be unique to each instance of a device.

PUFs based sustainable security solutions can mitigate cybersecurity vulnerabilities and the impacts of potential attacks in Internet-of-Things (IoT) and cyber-physical systems (CPS) that form the core of smart consumer devices, smart cities, smart healthcare, smart transportation, smart building, smart infrastructure, smart power grid and energy, and other emerging smart electronics paradigms [2-4]. We briefly introduce the accepted articles in the following paragraphs.

Electronic money or e-Cash is becoming increasingly popular as the preferred strategy for making purchases, both on- and off-line. The article *"Artificially Intelligent Electronic Money"* investigates several artificial intelligence (AI) approaches for improving performance and privacy within a previously proposed e-Cash scheme called PUF-Cash. PUF-Cash utilizes PUFs for authentication and encryption operations between Alice, the Bank and multiple trusted third parties (mTTPs).

Tracking the host carrying the virus of COVIS-19 has been one of the major issues during this pandemic. The article *"PIM: A PUF Based Host Tracking Protocol for Privacy Aware Contact Tracing in Crowded Areas"* proposes Physical Unclonable Function (PUF) based Privacy-aware Identification Module (PIM), an Internet of Medical Things (IoMT) architecture to track the host carrying the virus in a crowded area.

CPS integrates sensors, computing platforms, and networking among constituent blocks. To build hardware security primitives, e.g. True Random Number Generator (TRNG) and PUF from sensors and energy harvesting devices in CPS is a novel research direction. The article *"An Integrated TRNG-PUF Architecture based on Photovoltaic Solar Cells"* proposes integrated TRNG-PUF architecture devised around a common entropy source of Photovoltaic solar cell.

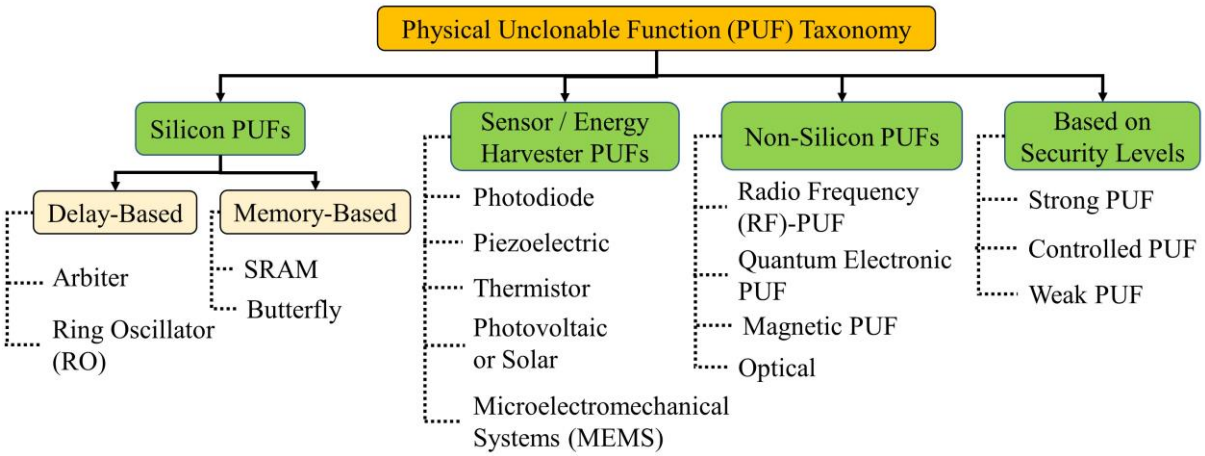

Figure 1. Classification of PUF Designs adapted from [1].

The article *"A Secure Hardware-Assisted AMI Authentication Scheme for Smart Cities"* proposes a hardware-assisted framework for AMI (advanced metering infrastructure) networks to achieve end-to-end key management and enable trusted and secure authentication in AMI systems. This framework utilizes low-cost and efficient PUFs with improved challenge-response pair (CRP) characteristics, namely, d-ROPUF (dynamic ring-oscillator PUF) to obtain a large number of authentication keys.

The guest editors sincerely believe that this Special Section will be good reading for Consumer Technology researchers around the globe. The guest editors would like to thank all the authors for their excellent contributions and the reviewers for their help in reviewing the manuscripts.

References:

[1] S. Joshi, S. P. Mohanty, and E. Kougianos, "Everything You Wanted to Know about PUFs", *IEEE Potentials Mag*, Vol. 36, Issue 6, November-December 2017, pp. 38--46.

[2] C. Labrado, H. Thapliyal, S. Prowell, and T. Kuruganti "Use of Thermistor Temperature Sensors for Cyber-Physical System Security", *Sensors*, Vol. 19, No. 18, 3905, 2019.

[3] S. P. Mohanty, V. P. Yanambaka, E. Kougianos and D. Puthal, "PUFchain: A Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in the Internet of Everything (IoE)," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 8-16, March 2020.

[4] A. Shamsoshoara, A. Korenda, F. Afghah, and S. Zeadally, "A survey on physical unclonable function (PUF)-based security solutions for Internet of Things," *Computer Networks*, vol. 183, p. 107593, Dec. 2020.

Guest Editors Bio:

Himanshu Thapliyal is an Associate Professor with the Department of Electrical and Computer Engineering, University of Kentucky, Lexington, KY, USA. Contact him at hthapliyal@uky.edu.

Saraju P. Mohanty is a Professor at the Department of Computer Science and Engineering, University of North Texas, Denton, TX, USA. Contact him at smohanty@ieee.org.