# Overview of PUF-Based Hardware Security Solutions for the Internet of Things

Basel Halak, Mark Zwolinski and M. Syafiq Mispan
ECS, University of Southampton, Southampton SO17 1BJ, UK
Email:{bh9, mz, msm1g14}@ecs.soton.ac.uk

***Abstract*—**The Internet of Things (IoT) consists of numerous inter-connected resource-constrained devices such as sensors nodes and actuators, which are linked to the Internet. By 2020 it is anticipated that the IoT paradigm will include approximately 20 billion connected devices. The interconnection of such devices provides the ability to collect a huge amount of data for processing and analysis. A significant portion of the transacted data between IoT devices is private information, which must not in any way be eavesdropped on or tampered with. Security in IoT devices is therefore of paramount importance for further development of the technology. Such devices typically have limited area and energy resources, which makes the use of classic cryptography prohibitively expensive. Physically Unclonable Functions (PUFs) are a class of novel hardware security primitives that promise a paradigm shift in many security applications; their relatively simple architecture can answer many of the security challenges of energy-constrained IoT devices. In this paper, we discuss the design challenges of secure IoT systems; then we explain the principles of PUFs; finally we discuss the outstanding reliability and security problems of PUF technology and outline the open research questions in this field.

***Abstract*—The Internet of Things (IoT) consists of numerous inter-connected resource-constrained devices such as sensors nodes and actuators, which are linked to the Internet. By 2020 it is anticipated that the IoT paradigm will include approximately 20 billion connected devices. The interconnection of such devices provides the ability to collect a huge amount of data for processing and analysis. A significant portion of the transacted data between IoT devices is private information, which must not in any way be eavesdropped on or tampered with. Security in IoT devices is therefore of paramount importance for further development of the technology. Such devices typically have limited area and energy resources, which makes the use of classic cryptography prohibitively expensive. Physically Unclonable Functions (PUFs) are a class of novel hardware security primitives that promise a paradigm shift in many security applications; their relatively simple architecture can answer many of the security challenges of energy-constrained IoT devices. In this paper, we discuss the design challenges of secure IoT systems; then we explain the principles of PUFs; finally we discuss the outstanding reliability and security problems of PUF technology and outline the open research questions in this field.**