CHIST-ERA Call 2015

Project: IDENTIFICATION IoT

Coordinator: Technische Universiteit Eindhoven (TU/e)

Participants: Boris Skoric (TU/e), Teddy Furon (INRIA Rennes), Sviatoslav Voloshynovskiy (University Geneve)

Summary:
The IoT will contain a huge number of devices and objects that have very low or nonexistent processing and communication resources, coupled to a small number of high-power devices. The weakest devices, which are most ubiquitous, will not be able to authenticate themselves using cryptographic methods. Other important tasks in the IoT will be to verify if an object is authentic, or to identify an object. Our plan is to address these issues using Physical Unclonable Functions (PUFs). PUFs, and especially Quantum Readout PUFs, are ideally suited to the IoT setting because they allow for the authentication and identification of physical objects without requiring any crypto or storage of secret information.
Furthermore, we foresee that back-end systems will not be able to provide security and privacy via cryptographic primitives due to the sheer number of IoT devices. Our plan is to address these problems using privacy-preserving database structures and algorithms with good scaling behaviour. Approximate Nearest Neighbour (ANN) search algorithms, which have remarkably good scaling behaviour, have recently become highly efficient, but do not yet have the right security properties and have not yet been applied to PUF data.
Summarised in a nutshell, the project aims to improve the theory and practice of technologies such as PUFs and ANN search in the context of generic IoT authentication and identification scenarios.