QUANTUM INNOVATION 2021

CC-03-04

Quantum physical unclonable functions and their comprehensive cryptanalysis

Elham Kashefi

CNRS Sorbonne Universite and University of Edinburgh

Abstract

A Physical Unclonable Function (PUF) is a device with unique behaviour that is hard to clone due to the imperfections and natural randomness during the manufacturing procedure, hence providing a secure fingerprint. A variety of PUF structures and PUF-based applications have been explored theoretically as well as being implemented in practical settings. Recently, the inherent unclonability of quantum states has been exploited to derive the quantum analogue of PUF as well as new proposals for the implementation of PUF. In this talk, we present the first comprehensive study of quantum Physical Unclonable Functions (qPUFs) with quantum cryptographic tools, introducing a new quantum learning attack that can explore the vulnerabilities of quantum and certain classical PUFs leading to general no-go results on the unforgeability of qPUFs. On the other hand, we prove that a large family of qPUFs (called unitary PUFs) can provide quantum selective unforgeability which is the desired level of security for most PUF-based applications. Moreover, we elaborate on the connection between qPUFs as hardware assumptions, and computational assumptions such as quantum pseudorandomness in order to establish the link between these two relatively new fields of research.