Cryptology ePrint Archive: Report 2013/084

Security of Quantum-Readout PUFs against quadrature based challenge estimation attacks

Boris Skoric and Allard P. Mosk and Pepijn W.H. Pinkse

Abstract: The concept of quantum-secure readout of Physical Unclonable Functions (PUFs) has recently been realized experimentally in an optical PUF system. We analyze the security of this system under the strongest type of classical attack: the challenge estimation attack. The adversary performs a measurement on the challenge quantum state in order to learn as much about it as he can. Using this knowledge he then tries to reconstruct the challenge and to emulate the PUF. We consider quadrature measurements, which are the most informative practical measurements known to us. We prove that even under this attack the expected number of photons detected in the verification mechanism is approximately a factor $S+1$ too low; here S is the Quantum Security Parameter, defined as the number of modes in the optical system divided by the number of photons in the challenge. The photon count allows for a reliable distinction between an authentic PUF and a challenge estimation attack.

Category / Keywords: PUF, quantum security, speckle

Date: received 18 Feb 2013, last revised 4 Mar 2013

Contact author: b skoric at tue nl