Cryptology ePrint Archive: Report 2013/215

Optical PUFs Reloaded

Ulrich Rührmair and Christian Hilgers and Sebastian Urban and Agnes Weiershäuser and Elias Dinter and Brigitte Forster and Christian Jirauschek

Abstract: We revisit optical physical unclonable functions (PUFs), which were proposed by Pappu et al. in their seminal first publication on PUFs [40, 41]. The first part of the paper treats non-integrated optical PUFs. Their security against modeling attacks is analyzed, and we discuss new image transformations that maximize the PUF's out- put entropy while possessing similar error correction capacities as previous approaches [40, 41]. Furthermore, the influence of us- ing more than one laser beam, varying laser diameters, and smaller scatterer sizes is systematically studied. Our findings enable the simple enhancement of an optical PUF's security without addi- tional hardware costs. Next, we discuss the novel application of non-integrated optical PUFs as so-called "Certifiable PUFs". The latter are useful to achieve practical security in advanced PUF-pro- tocols, as recently observed by Rührmair and van Dijk at Oakland 2013 [48]. Our technique is the first mechanism for Certifiable PUFs in the literature, answering an open problem posed in [48].

In the second part of the paper, we turn to integrated optical PUFs. We build the first prototype of an integrated optical PUF that functions without moving components and investigate its se- curity. We show that these PUFs can surprisingly be attacked by machine learning techniques if the employed scattering structure is linear, and if the raw interference images of the PUF are available to the adversary. Our result enforces the use of non-linear scattering structures within integrated PUFs. The quest for suitable materials is identified as a central, but currently open research problem.

Our work makes intensive use of two prototypes of optical PUFs. The presented integratable optical PUF prototype is, to our knowledge, the first of its kind in the literature.

Category / Keywords: Optical Physical Unclonable Functions (PUFs), Machine Learning, Implementation

Date: received 12 Apr 2013, last revised 10 May 2013

Contact author: ruehrmair at in tum de

Available formats: PDF | BibTeX Citation

Version: 20130510:065422 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]