Cryptology ePrint Archive: Report 2011/552

Recyclable PUFs: Logically Reconfigurable PUFs

Stefan Katzenbeisser, Ünal Kocabas, Vincent van der Leest, Ahmad-Reza Sadeghi, Geert-Jan Schrijen, Heike Schröder, Christian Wachsmann

Abstract: Physically Unclonable Functions (PUFs) are security primitives that exploit intrinsic random physical variations of hardware components. In the recent years, many security solutions based on PUFs have been proposed, including identification/authentication schemes, key storage and hardware-entangled cryptography. Existing PUF instantiations typically exhibit a static challenge/response behavior, while many practical applications would benefit from reconfigurable PUFs. Examples include the revocation or update of “secrets” in PUF-based key storage or cryptographic primitives based on PUFs.

In this paper, we present the concept of Logically Reconfigurable PUFs (LR-PUFs) that allow changing the challenge/response behavior without physically replacing or modifying the underlying PUF. We present two efficient LR-PUF constructions and evaluate their performance and security. In this context, we introduce a formal security model for LR-PUFs. Finally, we discuss several practical applications of LR-PUFs focusing on lightweight solutions for resource-constrained embedded devices, in particular RFIDs.

Category / Keywords: implementation / Logically Reconfigurable Physically Unclonable Functions (PUFs)

Publication Info: A preliminary version of this report that has been presented at CHES’11, and a more condensed version has been published in the Journal of Cryptographic Engineering. This version additionally provides detailed security proofs.

Date: received 6 Oct 2011, last revised 16 Jan 2012

Contact author: christian wachsmann at trust cased de

Available formats: PDF | BibTeX Citation

Version: 20120116:121841 (All versions of this report)

Discussion forum: Show discussion | Start new discussion
