Dokumenttyp: Report / Forschungsbericht

Autor(en): Merli, Dominik and Stumpf, Frederic and Sigl, Georg

Titel des Berichts: Protecting PUF Error Correction by Codeword Masking

Band / Teilband: Cryptology ePrint Archive, Report 2013/334

Abstract: One of the main applications of Physical Unclonable Functions (PUFs) is unique key generation. While the advantages of PUF-based key extraction and embedding have been shown in several papers, physical attacks on it have gained only little interest until now. In this work, we demonstrate the feasibility of a differential power analysis attack on the error correction module of a secure sketch. This attack can also be applied to code-offset fuzzy extractors because they build upon secure sketches. We propose a codeword masking scheme to protect key generation algorithms used for PUFs. Our proposed countermeasure enables masking of linear Error-Correcting Codes (ECCs) without impact on their error correction capabilities while keeping the overhead low. This is achieved by random masking codewords, which can be efficiently generated by the ECC’s encoding function. Further, it allows to consistently protect the PUF-based key generation process and can provide the masked key and its mask to a subsequent crypto module which implements masking as well. We demonstrate the practical protection of our codeword masking scheme by attacking a masked secure sketch implementation. We emphasize that, besides protecting code-offset algorithms, the proposed masking scheme can also be applied to index-based syndrome coding and other security-critical error correction modules.