Cryptology ePrint Archive: Report 2011/681

Physically Uncloneable Functions in the Universal Composition Framework

Christina Brzuska and Marc Fischlin and Heike Schr{\"o}der and Stefan Katzenbeisser

Abstract: Recently, there have been numerous works about hardware-assisted cryptographic protocols, either improving previous construction terms of efficiency, or in terms of security. In particular, many suggestions use Canetti's universal composition (UC) framework to model hardwa tokens and to derive schemes with strong security guarantees in the UC framework. Here, we augment this approach by considering Physically Uncloneable Functions (PUFs) in the UC framework. Interestingly, when doing so, one encounters several peculiarities specific to PUFs, such the intrinsic non-programmability of such functions. Using our UC notion of PUFs, we then devise efficient UC-secure protocols for basic tasks oblivious transfer, commitments, and key exchange. It turns out that designing PUF-based protocols is fundamentally different than for other hardware tokens. For one part this is because of the non-programmability. But also, since the functional behavior is unpredictable even for the creator of the PUF, this causes an asymmetric situation in which only the party in possession of the PUF has full access to the secrets.

Category / Keywords: cryptographic protocols / Universal Composition, Physically Uncloneable Function, Oblivious Transfer, Commitment, Exchange

Publication Info: "Physically Uncloneable Functions in the Universal Composition Framework" was published at CRYPTO 2011. This is the fu version.

Date: received 15 Dec 2011

Contact author: brzuska at cased de

Available formats: PDF | BibTeX Citation

Version: 20111218:161840 (All versions of this report)

Discussion forum: Show discussion | Start new discussion