On Error Correction for Physical Unclonable Functions

Sven Müelich

Institute of Communications Engineering,
Ulm University

Abstract

Cryptographic applications require random, unique and unpredictable keys. Since most cryptosystems need to access the key several times, it usually has to be stored permanently. This is a potential vulnerability regarding security, even if a protected memory is used as key storage. Implementing secure key generation and storage is therefore an important and challenging task which can be accomplished by Physical Unclonable Funtions (PUFs).

PUFs are, typically digital, circuits that possess an intrinsic randomness due to process variations which occur during manufacturing. They evaluate these variations and can therefore be used to generate secure cryptographic keys. It is not necessary to store these keys in a protected memory since they are implicitly stored in the PUF and can be reproduced on demand. However, the results when reproducing a key vary, which can be interpreted as errors. Thus, error correction must be used in order to compensate this effect.

We explain how methods from coding theory are applied in order to ensure reliable key reproduction. Previous work on this topic used standard constructions, e.g. an ordinary concatenated scheme of a BCH and Repetition code. Based on this work we show how better results can be obtained using code classes and decoding principles not used for this scenario before. We exemplify these methods by specific code constructions which improve existing codes with respect to error probability, decoding complexity and codeword length. Examples based on Generalized Concatenated, Reed–Muller and Reed–Solomon codes are given.