Konferenzbeitrag

Vortrag / Präsentation

Hiller, Matthias and Kürzinger, Ludwig and Sigl, Georg and Müelich, Sven and Puchinger, Sven and Bossert, Martin

Low-Area Reed Decoding in a Generalized Concatenated Code Construction for PUFs

Physical Unclonable Functions (PUFs) enable secure key storage for integrated circuits and FPGAs. PUF responses are noisy such that error correction is required to generate stable cryptographic keys. One popular approach is to use error-correcting codes. We present an area-optimized VLSI implementation of a recent Generalized Concatenated (GC) code construction using Reed–Muller codes. Reed–Muller codes have the advantage that there exist very efficient decoders. Our new Reed decoding implementation makes extensive use of a circular shift register. The functionality is extended so that it can also handle erasure symbols to improve the error correction capability. The overall GC code decoder occupies less than 110 slices and two block RAMs on an entry-level FPGA, and has a key error probability of $1.5 \times 10^{-9}$. The slice count is reduced by 50% compared to the reference implementation.

Physical Unclonable Functions (PUFs), Error Correction, Generalized Concatenated Codes, Reed–Muller Code, Reed