Dokumenttyp: Konferenzbeitrag

Art des Konferenzbeitrags: Vortrag / Präsentation

Autor(en) des Beitrags: Delvaux, Jeroen and Gu, Dawu and Verbauwhede, Ingrid and Hiller, Matthias and Yu, Meng-Day (Mandel)

Titel des Beitrags: Efficient Fuzzy Extraction of PUF-Induced Secrets: Theory and Applications

Abstract: The device-unique response of a physically unclonable function (PUF) can serve as the root of trust in an embedded cryptographic system. Fuzzy extractors transform this noisy non-uniformly distributed secret into a stable high-entropy key. The overall efficiency thereof, typically depending on error-correction with a binary \([n, k, d]\) block code, is determined by the universal and well-known \((n - k)\) bound on the min-entropy loss. We derive new considerably tighter bounds for PUF-induced distributions that suffer from, e.g., bias or spatial correlations. The bounds are easy-to-evaluate and apply to large non-trivial codes, e.g., BCH, Hamming and Reed-Muller codes. Apart from an inherent reduction in implementation footprint, the newly developed theory also facilitates the analysis of state-of-the-art error-correction methods for PUFs. As such, we debunk the reusability claim of the reverse fuzzy extractor. Moreover, we provide proper quantitative motivation for debiasing schemes, as this was missing in the original proposals.

Stichworte: