Formalism to assess the Loop-PUF entropy and reliability

J-Luc Danger, O. Rioul, S.Guilley
Telecom ParisTech
France

Abstract

Many Methods exist for Physically Unclonable Function in order to enhance their reliability, but they are at the cost of extra hardware, either coming from the PUF core itself, or from the correction method, as fuzzy extraction [5]. Another issue is to better know the PUF entropy, especially when the PUF is used as a cryptographic key generator. The SRAM and Ring Oscillator PUF provide relatively high entropy, as shown experimentally in [4]. The min-entropy is generally better assessed, as studied in Delvaux et al. [2] which presents the min-entropy of strong PUFs. For strong PUFs, it appears that the number of required challenges to get the min-entropy is signifficantly higher, thus involving compression and extra complexity to generate key bits. We show in this study that it is possible to obtain a strong PUF, relying on a Loop PUF, which presents a high ratio between reliability and complexity. Moreover the entropy can be known when choosing the minimal and optimal number of challenges, namely Hadamard Codes. As the presence of noise inevitably involves an entropy decrease, this paper presents a method allowing the PUF to compensate this loss to meet the requires entropy. The single Ring-Oscillator of the Loop PUF, the hard-coded challenges and the lightweight error correction provide a low complexity PUF, around 1000 μm^2 , with an access time of 20 ms to get a 64 key bits with a Bit Error Rate (BER) which can be less than 10^{-9} by filtering unreliable bits. As the challenges and responses remain local, the modeling attacks are signiffificantly reduced and are not considered in this work.