12

On the Amount of Entropy in PUFs©

Boris Škorić and Pim Tuyls

12.1 Introduction

The aim of this chapter is to provide an information-theoretic framework for the analysis of physical unclonable function (PUF) security. We set up this framework and then apply it to optical PUFs and coating PUFs. From the description of PUFs in Chapter 1 some obvious questions arise in the context of the security primitives discussed in Part I.

• How much information does a PUF contain?
• How much of this information can be used for security purposes?
• How hard is it for an attacker to extract enough information to launch an effective attack?
• How do we define a quantitative security parameter?

We address the first two questions by introducing the notions of “intrinsic entropy,” “measurement entropy,” and “measurable entropy.” All of these entropies depend on the random process of creating the PUF. In addition, the latter two also depend on the resolution of measurements. The intrinsic entropy is the entropy of the PUF creation process. The measurement entropy (also referred to as response entropy) gives the lack of knowledge about the outcome of a single (predetermined) measurement. The measurable PUF entropy does the same, but for all possible combinations of “relevant” measurements. By “relevant” we mean those measurements that are relevant for the operation of the security system. For instance, if the installed challenging devices probe PUF structures down to a length scale of a micrometer, then sub-micrometer measurements are not relevant. Hence, even though a PUF may contain an infinite amount of information, the amount that can actually be used, the measurable entropy, is limited by the resolution of the measurements.

To address the last two questions, we work with the following attack model. The PUF is unprotected, meaning that there is no access control of the type discussed in Chapter 14, but it takes finite time to perform a measurement. The attacker gets hold of the PUF for a finite amount of time. (For instance, while the owner of the PUF is sleeping or otherwise unable to notice the attack.) During this time, the attacker subjects the PUF to as many challenges as he can and stores the Challenge-Response Pairs (CRPs) in a database. He is allowed to do so in an adaptive way. We assume that the attacker has infinite computation power. We say that the attack is successful if the obtained information enables him to predict, with significant probability, the response to a new random challenge.

We define the PUF security parameter $C$ as the maximum number of independent CRPs. We call a set of CRPs independent if none of the responses can be predicted, in the information-theoretic sense, from the other CRPs in the set. From the maximum set of independent CRPs, all responses can be predicted in theory. Hence, we have an information-theoretic security parameter, representing the minimum number of measurements that is required for the computationally unbounded adversary to extract all measurable entropy from the PUF. (For a computationally bounded adversary, the attack is, of course, much harder, especially if the interactions in the PUF are complex.) Assuming equivalence of all responses, we show that $C$ is given by the ratio of measurable entropy and measurement entropy.

Our framework can be applied to all types of PUF. In Sections 12.3 and 12.4 we analyze the case of optical PUFs and coating PUFs. For optical PUFs, the measurable entropy is easily estimated as the number of “voxels” (wavelength-sized cubes) in the PUF. The response entropy is computed using the waveguide model of multiple scattering and the quantization of light [272]. The security parameter is typically of order $10^4$ per square millimeter of PUF surface.

The situation is completely different for coating PUFs. For one sensor and one challenge frequency, there is only one possible measurement. The measurable entropy is equal to the measurement entropy when there is almost no noise, and $C = 1$. Hence, a coating PUF should never be unprotected, but used as a controlled PUF (see Chapter 14). The extracted key is sometimes referred to as a physically obfuscated key (POK). The POK entropy is equal to the measurement entropy. We compute the measurement entropy in a simplified parallel-plate model, where the dielectric particles are cubes on a grid. We distinguish between two cases: noiseless and noisy measurements. In the noiseless case, the measurable entropy is equal to the measurement entropy. We show how to partition the PUF space into equivalence classes of equal capacitances. In the noisy case, the measurement entropy is determined by the signal-to-noise ratio, where the “signal” is the variance of the capacitance. When the particles are made smaller, the measurable entropy grows, but the noisy measurement entropy decreases due to averaging effects. Because of these counteracting trends, there is (at fixed noise power) an optimum particle size where the measurement entropy is maximal. We study this optimal point.