Characterisation of Physically Unclonable Functions at Design Stage

Zouha CHERIF JOUINI¹², Jean-Luc DANGER², Lilian BOSSUET¹
¹ Université de Lyon, CNRS, UMR5516, Laboratoire Hubert Curien 42 000 Saint-Etienne, France
² Institut TELECOM, TELECOM ParisTech, CNRS LTCI, 46 rue Barrault 75 634 Paris, France.
{lilian.bossuet@univ-st-etienne.fr, {cherif,danger}@telecom-paristech.fr}

Abstract—The evaluation of Physically Unclonable Function (PUFs) quality is an open problem, as the PUF represents a circuit signature which depends on process variation but also environmental conditions. Some metrics consisting in analysing the statistics of PUF outputs have been introduced. The considered metrics are often the randomness (max entropy), the uniqueness (two PUFs should be different), and the steadiness (Reliability of the result). The drawback of this statistical analysis is that the silicon is necessary, thus involving a long and costly chip manufacturing process without the certainty to obtain a high-quality PUF. The objective of our research topic is to propose a new method which allows to evaluate a silicon PUF, based on delay elements, at design stage without the need to have the circuit. The essence of the method is based on a Monte-Carlo simulation of the netlist in order to take into account the process variation and the environment. To be validated, this method requires a comparison between the simulation results and measurements on silicon. The first step of the study, which is presented in this paper, is to redefine the metrics in order to run Monte-Carlo simulation on delay elements.

Thus the randomness, uniqueness and steadiness metrics are revised and expressed in term of probabilities. Experiments have been carried out to extract the metrics from measurements on CYCLONE II FPGAs with different PUF structures. Hence these metrics are used two compare the Arbiter PUF (APUF) and Loop PUF (LPUF) in order to validate their soundness.

Keywords: Physically Unclonable Function (PUF); Silicon PUF, PUF metric, 65nm technology, FPGA.

I. INTRODUCTION

A Physically Unclonable Function (PUF) is a function which returns a value characteristic of an integrated circuit (IC). This device signature can be used to control the local behaviour of an algorithm. For instance cryptographic applications take advantage of PUF for authentication or key generation purposes. The Silicon PUF outputs a response (or ID) which depends on a control word, called the “challenge”. A simple device authentication is based on a “challenge/response pair” which is the association between a set of challenges and the responses returned by a PUF. Due to the dispersion of the manufacturing process, the response for a given challenge be different between PUFs. Among the variety of PUF, the Silicon PUF is certainly the simpler to design as it does not require any specific technology. There are two main classes of Silicon PUFs: the PUFs based on delay comparisons, composed of identical elements, and the PUFs exploiting the initial state of memory blocks. The first silicon PUF introduced by Gassend & al is the Arbiter PUF [2] which compares the delay between two identical control paths. The Arbiter PUF can be derived to XOR PUF suggested in [7], and Lightweight Secure PUF [6], and Loop PUF [4] which is a composition of Arbiter PUFs. This paper deals with PUFs based on delay chain comparison as arbiter PUFs, loop PUFs.

To perform an efficient characterization of PUFs, at least three metric are necessary: randomness, uniqueness and steadiness. The randomness gives an estimate of the imbalance between the number of IDs at ‘0’ and the IDs at ‘1’ for all the challenges. The uniqueness indicates the entropy between two PUFs, either in the same device (intra-uniqueness) or between devices (inter-uniqueness). The steadiness expresses the level of PUF reliability which is decayed by the noise coming from the measurement environment.

There two types of methods to characterize the PUFs. The first type is that of classical methods. They require to perform statistical tests as those proposed in [3]. These methods consider the set of logical PUF IDs. Hence, they need a lot of trials in order to run a Monte-Carlo estimation method. The second type is that of the fast method, proposed in [1]. It is based on the measurement of the physical values, i.e., the delays or frequencies. The advantage of this method is that only the number of tests is linear in M, where M is the number of elements composing the PUF. In our work, we consider the fast method.

II. BACKGROUND

In this section, we, first describe the structure of used PUF, Arbiter PUF and Loop PUF. Then, we present metric considered to evaluate PUFs.

A. Arbiter PUF

The example structure of the Arbiter PUF is made up of M identical delay elements structured as a mini crossbar 2x2, as illustrated in Figure[1]. A step input simultaneously triggers the two paths which are controlled by a control word C, or challenge. At the end of the two parallel paths, a flip-flop D is used to convert the analog delay difference between the paths to a digital value which represents the response ID. Although the two paths are built identically, due to their intrinsic CMOS variation, the delays of the two selected paths are different. Therefore, the Arbiter PUF is expected to output unique IDs to the device.
The arbiter PUF can be designed using two delay chains of $M$ elements (Figure 2) as presented in [1].

**B. Loop PUF**

As presented in [4], the "Loop PUF" is a silicon PUF based on $N$ delay chains forming a loop. When closed by an inverter this loop oscillates as a single ring oscillator. A delay chain is composed of $M$ controlled delay elements shown in Fig. 2. Every delay chain $i$ receives a control word $C_i$ of $M$ bits. Each bit $C_{ij}$, $i \in [1, N]$, $j \in [1, M]$, selects a delay value of the associated $j$ delay element in the chain $i$.

![Figure 2. A structure of a delay element](image)

**C. Used metric to evaluate PUFs**

The base of the PUF metric is to calculate a probability that expresses the quality to be random, unique or reliable. Arbiter and Loop PUF metric are explained in [1] and [4]. For instance, metric used for arbiter PUFs are presented below:

**Randomness:**

\[
\text{Randomness} = 1 - |Pr(ID = 0) - Pr(ID = 1)|. \tag{1}
\]

**Uniqueness:** If we consider $L$ PUFs, the global normal distribution $D$ has $M \cdot L$ elements. We have to compare the $M$ distributions $D_i^L$, $i \in [1, M]$, with the global distribution $D$.

\[
\text{Uniqueness} = \frac{1}{M} \sum_{i=1}^{M} Pr(D_i^L = D). \tag{2}
\]

**Steadiness:** It is merely the opposite of the error probability:

\[
\text{Steadiness} = 1 - Pr(error). \tag{3}
\]

**III. EXPERIMENTS ON FPGAS**

Tests have been carried out in a CYCLONE II EP2C35F672 FPGA with $L=16$ for the Arbiter PUFs and $L=8$ for the Loop PUF. In both studied PUFs, there are $M=8$ delay elements per delay chain.

**A. Results**

Results of the intra-device evaluation of Arbiter PUF and Loop PUF are presented in Table 1.

<table>
<thead>
<tr>
<th>Performance indicator</th>
<th>Arbiter PUF</th>
<th>Loop PUF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Randomness</td>
<td>0%</td>
<td>≈ 100%</td>
</tr>
<tr>
<td>Intra-Uniqueness</td>
<td>97.73%</td>
<td>95%</td>
</tr>
<tr>
<td>Steadiness</td>
<td>99.07%</td>
<td>98.7%</td>
</tr>
</tbody>
</table>

Table 1 reveals that the implemented PUF is absolutely not random (0%) on the contrary to The Loop PUF which is naturally random. This shows that the bias of the two independent delay lines has a lot of impact, as explained in [5], where a delay is introduced to compensate this bias. Both Arbiter and Loop PUFs have good intra-Uniqueness and steadiness properties. However the steadiness should be estimated in other temperature and voltage configurations to cover all the conditions. The steadiness metrics gives a good idea of the capacity of the necessary error correction code to enhance the reliability towards 100%.

**IV. CONCLUSION**

In this paper, a novel approach to characterize PUFs on design stage has been presented. Tests on FPGAs has been realized to validate this approach before applying it for ASIC design. Experiments have been carried out on CYCLONE II FPGAs. The results show that the Loop PUF is much more random than arbiter PUF. However, both present a good percentage in terms of uniqueness and reliability.

Future work include the application of this approach to characterize the quality of a combined PUF design using Monte-Carlo simulation for process variation and Spectre simulator options for environmental variation.

**REFERENCES**