Ring Oscillator PUF on FPGA: Design and Characterisation by Using Second-Order Compensated Measurement

Jorge Fernandez-Aragon[1], Guillermo Diez-Señorans[1], Miguel Garcia-Bosque[1,2], Santiago Celma[1]

[1] Grupo de Diseño Electrónico (GDE) - Instituto de Investigación en Ingeniería de Aragón (I3A)
[2]Centro Universitario de la Defensa de Zaragoza
e-mail: 704364@unizar.es

Abstract

Physically unclonable functions (PUFs) have become an important area of study in the field of hardware security. In this paper we will design ring oscillator PUFs implemented in FPGAs and characterise them using a new concept: second-order compensated measurement by two-bit extraction.

Introduction

The great advance of technologies and their increasingly extensive use in our daily lives allow us to share information quickly and easily with all types of users and entities throughout the world. This information is often intended to be confidential and inaccessible to third parties. To make this possible, different solutions such as identification numbers (IDs) or more recently physically unclonable functions (PUFs) are used [1]. A physically unclonable function (PUF) is an entity that uses the stochastic variations inherent to manufacturing process in the output to create a device-specific response that is usually digitized into binary format. In a generic way it could be seen as the "fingerprint" of the device. These entities have the properties of being identifiable and physically unclonable [2]. While there are different alternatives for their implementation in both ASICs and FPGAs (Field Programmable Gate Arrays), in this work, we will focus on the design and characterisation of a ring oscillator PUF (RO-PUF) implemented in FPGA which employs the second-order compensated measurement. This approach is novel, and our aim is to show that this technique might be used to boost the performance of RO-PUF regarding entropy per area production.

Properties of PUF

Reproducibility: This property implies that if a PUF is reproducible, any of its instances will always have the same response to the same stimulus. Intra-distance is used to measure the difference in the response of a particular instance of a PUF to the same challenge.

Uniqueness: For the same stimulus, the response of different instances of the PUF is expected to be very different. This property is measured by inter-distance. Both intra-distance and inter-distance are typically measured using the Hamming Distance, which shows the number of different positions between two vectors of equal length. If the PUF response is a n-bit word, $x = (x_1, x_2, \dots, x_n)$, the Hamming Distance (HD) between two responses x, x' is defined as:

$$HD = \sum_{i=1}^{n} x_i \oplus x'_i \quad (1)$$

where $\oplus$ stands for the XOR operation.

Identifiability: A PUF has the property of identifiability if its instances can be identifiable, which implies that the properties of reproducibility and uniqueness are fulfilled [3]. Of course, a PUF does not need to have perfect reproducibility and uniqueness, since in practice it is almost impossible to achieve intra-distances equal to 0% and inter-distances of exactly 50% (these are ideal average values). Inter- and intra- Hamming distances are distributed like binomial distributions around their respective average values. The necessary condition for a PUF to be identifiable is that the intra-distance is smaller than the inter-distance to a high probability degree (Fig 1).

Physically unclonable: This fact implies that the PUF manufacturing process cannot be influenced, which means that no two instances with the same or similar behaviour can be created. This property is unique of PUFs compared to other cryptographic primitives.

Methodology and implementation

In this work we will use the minimal (3-inverter) RO-PUF implemented in an FPGA, where we will use as an identifier the frequency differences that occurs

between a set of ring oscillators equal in design but with small differences caused by stochastic variations occurred during the manufacturing process. This way, we will extract the number of cycles of the ring oscillators, measured over a certain number of clock cycles, i.e., their characteristic frequency. To obtain the binary response, we will compare the frequencies of pairs of oscillators so that we can construct a 32-bit array, whose first bit (the most significant) will be a 0 or a 1 depending on whether the difference is positive or negative (i.e., the sign of the difference), and the remaining 31 bits will be the result of the subtraction converted to a binary number (Fig 2a). Compensated measurement is a technique that normally uses the sign bit [4] and, in this work, we will use an additional bit extracted from the difference between frequencies, to create a second order binary response twice the length. To obtain the binary response we will use a Zynq 7000 SoC on which we will implement an array of 51 ring oscillators, thus obtaining 50-bit words by comparing consecutive oscillators [5]. Each oscillator is composed of 3 inverters and an AND logic gate. We will repeat this architecture in 20 different positions of the FPGA (Fig 2b), thus simulating different PUF instances and we will repeat the measurements 58 times to have some statistic. Each 50-bit word will be a succession of zeros and ones corresponding to the bit we select in each case within the 32-bit array formed by the frequency comparison, we can extract the inter-distance and intra-distance for each bit and thus obtain the binary response. In order to test the reliability of a PUF, the response generated by an entity must be compared with the intra-distance and inter-distance threshold, thus generating four possible scenarios [2]. In our case, we will focus on false acceptance and false rejection which will be modelled respectively, by the false rejection rate (FRR) and the false acceptance rate (FAR). We can also plot both parameters to obtain the receiver-operating characteristic (ROC) plot of the system. With these metrics we can find a suitable balance that meets the requirements of the application.

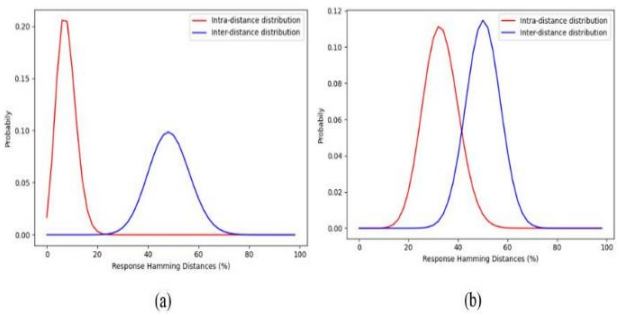

Fig. 1 Intra-chip Hamming Distance and inter-chip Hamming Distance distributions with: (a) high identifiability and (b) low identifiability.

Results

As already known, the bit obtained with the sign of the difference (standard RO-PUF) gives us mean inter-distance values with a binomial distribution close to 1% and very close to 50% for the intra-distance. In addition, promising results have been obtained for other candidate bits from the digitized comparison, with mean intra-distances of 2% and mean inter-distances close to 50%. This leads us to believe that it is possible to obtain a second-order compensated measurement capable of extracting two bits out of a single comparison, thus potentially duplicating the entropy extracted from RO-PUF.

Conclusions

In this work we have designed and characterised RO-PUF implemented in FPGA, by using a novel technique called second-order compensated measurement. For this purpose, we have compared the oscillation frequency between pairs of oscillators, being capable of obtaining two high quality bits from the difference and thus achieving improved PUF throughput, e.g., reducing the PUF area up to twice compared to standard RO-PUF.

REFERENCES

[1]. HOFER, Maximilian and Christoph BÖHM. 2013. Physical Unclonable Functions in Theory and Practice. 1. Aufl. edn. Anon. New York, NY: Springer. ISBN 9781461450399.

[2]. MAES, Roel. 2012. Physically Unclonable Functions: Concept and Constructions. En: Anon. Physically Unclonable Functions. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN 9783642413940.

[3]. GARCIA-BOSQUE, M., et al. Sep 2020. Introduction to Physically Unclonable Fuctions: Properties and Applications. 2020 European Conference on Circuit Theory and Design (ECCTD). pp 1-4.

[4]. DÍEZ SEÑORANS, G., et al. ISSN 2341-4790. 2019. Implementación De Arquitectura ROPUF En FPGA Para Identificación Segura De Dispositivos. Jornada de Jóvenes Investigadores del I3A. 7.Boletín Oficial del Estado, 26 de febrero de 2009, núm. 49, pp. 19893-20016.

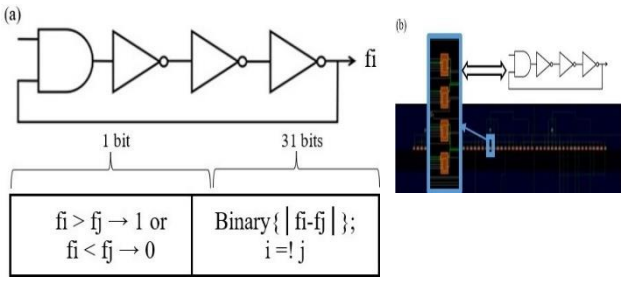

Fig. 2. Diagrams of the composition and distribution of the ring oscillators: (a) Ring oscillators with three inverters and an AND gate that returns their oscillation frequency with which we generate a 32-bit array. (b) Distribution of the array of 51 ring oscillators and the 20 PUFs within the same FPGA.