A New Approach to Analysis the Security of Compensated Measuring PUFs

G. Díez-Señorans, gds@unizar.es
M. Garcia-Bosque, mgbosque@unizar.es
C. Sánchez-Azqueta, csanaz@unizar.es
S. Celma, scelma@unizar.es

Group of Electronic Design, University of Zaragoza
Zaragoza, Spain

***Abstract* - In this paper we perform an entropy analysis and probability distribution analysis over simulated PUFs operating under a compensated measuring digitization scheme. The behavior of the PUFs have been simulated by generating a set of pseudorandom numbers uniformly distributed, which simulate the measured parameters, using the definition of the so called "topology of the PUF", i.e. the way in which different parameter measurements are compared to obtain a digital binary output. At this respect, we prove the existence of a shortcoming in the most commonly used PUF topologies. as well as provide some guidelines to overcome it.**

Keywords - Physically Unclonable Function (PUF), entropy, compensated measuring, ring oscillator.

I. Introduction

Physically Unclonable Functions (PUFs) are a developing alternative to ensure cryptographic security in systems whose physical support is intended to be out of control (portable devices, internet of things, etc), and thus vulnerable to physical attacks such as invasive and side channel attacks [1], [2], [3], [4], [5]. Electronic PUFs are understood as pieces of hardware which provide a digital response when exposed to a suitable stimulus. Traditionally PUFs have been classified depending on the size of this stimuli space as either weak if it is small (i.e. it can be exhausted in polynomial or less time) or strong (otherwise) [3]; however it has been proved by some authors [4] that the amount of information within a given space is upperly bounded by fundamental physical arguments [6] to be asymptotically polynomial on the physical parameters of this space, thus deprecating the "classical" definition of weak/strong PUFs in terms of complexity theory. For the sake of simplicity on this communication we will attach to the "weak/strong" terminology in the sense that the challenge space of a strong PUF will not be exhausted in a reasonable amount of time, while weak's might be.

As a consequence of this intrinsic difference, both types of PUFs behave in a dramatically different way, and thus they find application in very different fields: weak PUFs (also called Physical Obfuscated Keys) provide a secure key "storage" mechanism in which keys are re-generated from hardware-specific features of the device rather than stored in non-volatile memories [1], [2], [3], while strong PUFs can be used in identification/authentication protocols as well as key generation [3], [5]. However, in the last few years some work has been made in proving a number of believed strong PUFs (e.g. arbiter PUF, XOR arbiter PUF, etc) to be vulnerable to machine learning driven modeling attacks, since this kind of PUFs usually lack of a limitation in the number of stimulus-response pairs (usually called "challenge-response" pairs, *CRP*) that an adversary can harvest [7].

In this paper, a new method to asses the security of PUFs based on a statistical entropy analysis has been proposed. This method is of application to any type of PUF whose digitization procedure is based on compensated measuring [5], i.e. pair comparison of responses extracted from identically designed hardware; the main example of this scheme is the ring oscillator PUF (RO-PUF).

The methodology developed in this paper has been used to compare the security of three different well-known topologies of RO-PUFs: *1-out-of-2*, *N-1*, and *All-pairs*. Finally, a new topology, called *k-modular* has been introduced and compared with the previous ones. The entropy analysis shows that this new topology presents some clear advantages with respect to the previous architectures.

II. Background

Given an implementation of a matrix of ring oscillators, there exists a number of measurement protocols which affects dramatically the performance of this system as a PUF. These protocols are designed to obtain a digital binary response from an intrinsically analog system such as a matrix of frequency-meters, and are based on the comparison of pairs of ring oscillators a, b in such a way that the system deploys a "0" if $a < b$, or "1" otherwise [9], [10]. From now on we will refer to the specific way in which pairs of oscillators are compared as the *topology* of the RO-PUF instance; given N different oscillators there could be a total of $N(N-1)/2$ comparisons, which however will show some degree of correlation because of the transitive property of the ordering operation,

$$a < b \wedge b < c \longrightarrow a < c \tag{1}$$

Authorized licensed use limited to: Universidad de Zaragoza. Downloaded on December 11,2020 at 09:07:19 UTC from IEEE Xplore. Restrictions apply.

The least upper bound to the entropy of such a system is known to be $\log_2 N!$ bits [2], which can be easily understood considering that since bits are generated from comparison of frequency-meters, the actual value of the measured frequencies are irrelevant: the state of the system is specified by the frequency-ordered array of oscillators only, thus it follows that every single state of the system can be constructed by changing the order of the oscillators; since there are $N!$ different ways of ordering the array, information theory dictates that the entropy of the system (i.e. the maximum extractable entropy) is given by $\log_2 N!$ bits, which is obvious from the fact that a trivial outcome from such a system would be the ordering number of a specific implementation; since there are $N!$ different possible orderings there exist $N!$ different possible outcomes, which require $\log_2 N!$ bits to be specified. Nevertheless, the implementation of a topology which maximizes the number of independent bits extracted from this kind of system is complex and chip-dependent, which at the end of the day turns out to leave two main design options, as reviewed in the literature: the so called *1 out of k* topology [2], [5], [11], and the *N-1* bits topology [12]. The first of these takes one bit out of k different oscillators without repetition, by selecting the pair whose characteristic frequencies are further apart from each other. This scheme presents some advantages as it helps to strengthen the system against environmental variations (particularly temperature changes), at the cost of a large lost in performance since the extracted entropy per oscillator ratio decreases by a factor of k. On the other hand, the *N-1* bits strategy is an attempt to maintain the system within reasonable limits of environmental-robustness by performing comparisons between adjacent oscillators, while increasing the entropy outcome to approximately N bits.

III. Measuring setup

In this work we will investigate the probability distributions that emerge from different topologies $\mathcal{T}$ when applied to a set of M numerically simulated frequency arrangements, $\{\Omega^i\}_{i=1}^{M}$. Each of this frequency arrays Ω^i represents a different RO-PUF realization and contains N random numbers,

$$\left\{\omega_j^i \middle|\ \omega_j \in \Omega^i\right\}_{j=1}^{N}, \quad 0 < \omega < 1 \tag{2}$$

which emulate the frequency measurement of each oscillator within the specific instance. Thus the numerical apparatus Eval that we designed takes two parameters $\mathcal{T}$ and $\{\omega_j^i\}$, and produces a probability distribution $p(x)$ of the RO-PUF outcome,

$$\text{Eval}: \quad \mathcal{T},\ \{\omega_j^i\} \longrightarrow p(x), \quad 0 < x < 2^{N_{\text{bits}}} - 1 \tag{3}$$

In plain words, the system evaluates each frequency array according to the instructions provided by a specific topology, obtaining a binary word. The numerical experiment for each topology is carried out over a set of ten million different arrays. Once all binary words have been recovered, they are converted into decimal numbers (for the sake of statistical analysis) and used to construct the histogram that approximates the distribution $p(x)$ of the underlying system.

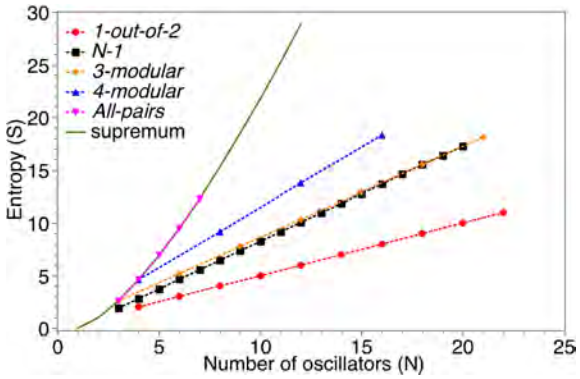

Figure 1. Total entropy for each topology analyzed against the number of oscillators.

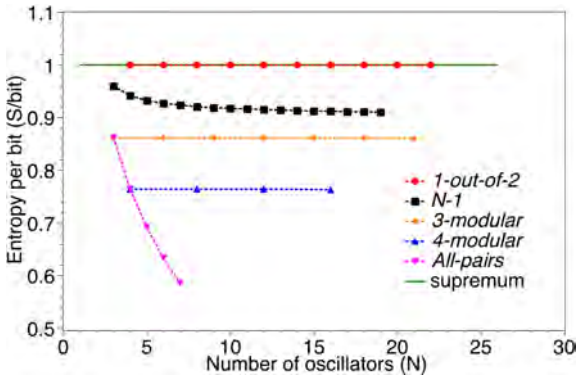

Figure 2. Entropy per bit ratio against the number of oscillators.

From these distributions we extract a number of interesting metrics which have been used as figures of merit: the entropy per bit ratio $S/_{\text{bit}}$ in Fig. 2 might be used to characterize resistance against cryptanalysis, while the entropy per oscillator ratio $S/_N$ in Fig. 3 influences performance regarding area and power consumption. Additionally the total Shannon entropy S and the product $S^2/_{N\cdot\text{bit}}$ are shown in figures 1 and 4 respectively. All these figures are presented all along with the supremum value (green line) for each metric.

In the next section, we will show the probability distributions obtained for different topologies, proving these to be non-uniform, indicating a potential weakness for this kind of PUFs whose digitization system is based in pairs comparison.

IV. Numerical results

In our research we have explored four different topologies:

A. 1-out-of-2

In this topology, each bit is obtained by comparing two adjacent oscillators without repetition, i.e. i and $i+1$ oscillators produce the $\frac{i}{2}$-th bit, thus $N/2$ bits are extracted from N oscillators. This kind of digitization and others within the *1-out-of-k* family (which are expected to behave in a similar way) are the most common topologies found in literature. It produces a plain distribution (Fig. 5) because of the lack of repetition in oscillators comparison, i.e. a high entropy per bit

Authorized licensed use limited to: Universidad de Zaragoza. Downloaded on December 11,2020 at 09:07:19 UTC from IEEE Xplore. Restrictions apply.

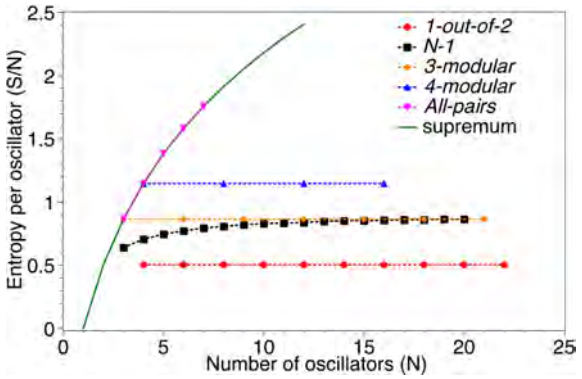

Figure 3. Entropy per oscillator ratio against the number of oscillators.

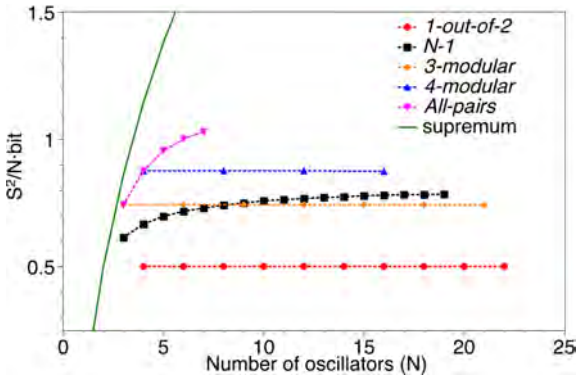

Figure 4. $S/_{\text{bit}} \times S/_{N}$curve for each topology analyzed. This quantity can be used as figure of merit as intends to comprise both entropy per bit and entropy per oscillator ratio within a single curve.

ratio (~ 1, see red dotted line in Fig. 2) which however comes at the cost of a poor entropy per oscillator ratio of $\sim 1/2$, red dotted line in Fig. 3. This results suggest that this topology is a deeply conservative one, thus useful on systems without power or area restriction, but might be of less use on mobile and wireless devices.

B. N-1 topology

In this topology $N-1$ bits are extracted from N oscillators by comparing oscillators i and $i+1$ in order to obtain the i-th bit, $1 \leq i \leq N-1$. This topology suffers a shortcoming that arises from the fact that the PUF is trying to accommodate $N!$ states on $N-1$ bits (which have room for 2^{N-1} different states, see Fig. 6), i.e. there exists some permutations of oscillators that leave invariant the comparison pattern between oscillators pairs, thus leading to identical outcomes for two different PUF realizations. If managed carefully, an adversary could take some advantage from this collision probability, for example by presenting fraudulent keys cleverly chosen in a probability-descendant way: it would be expected that such an adversary would succeed in impersonating the legit PUF much faster than one trying to exhaust the space of keys in a random fashion (yet further research in this direction is necessary). The total entropy as a function of the number of oscillators was found to be linearly dependent (see black dotted line at Fig. 1), while entropy per bit (Fig. 2) and entropy per oscillator (Fig. 3) evolves to saturation.

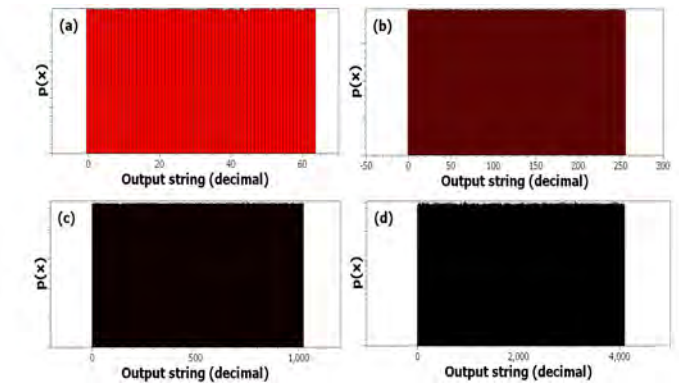

Figure 5. Outcome distribution for *1-out-of-2* topology: *(a)* $N = 12$, (b) $N = 16$, (c) $N = 20$, (d) $N = 24$.

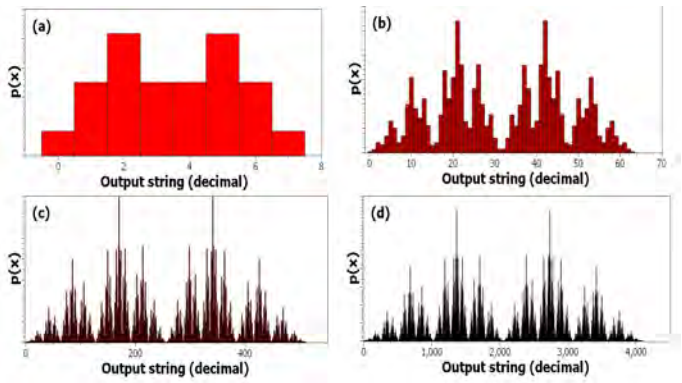

Figure 6. Probability distribution for different number of oscillators under *N-1* topology: *(a)* $N = 4$, (b) $N = 7$, (c) $N = 10$, (d) $N = 13$.

C. All-pairs topology

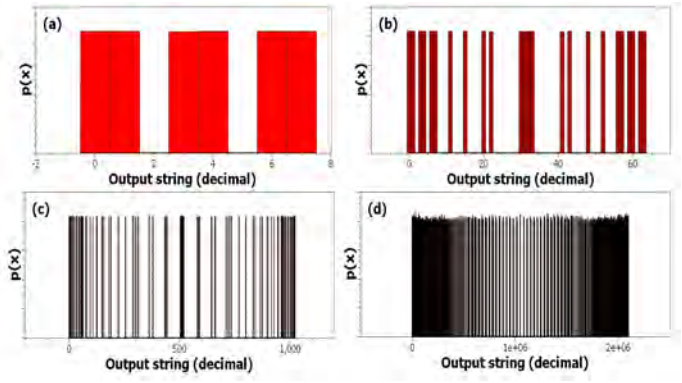

Figure 7. *All-pairs* probability distribution for different number of oscillators N: *(a)* $N = 3$, (b) $N = 4$, (c) $N = 5$, (d) $N = 7$.

In this case digitization process is carried out by exhausting all possible comparison in the matrix of oscillators, thus $N(N-1)/2$ pair bits are deployed. This way of extracting strings from the RO-PUF is infrequent in literature, since it suffers from a deep correlation as stated by expression 1. However, we have found it interesting to include it in our work for the sake of completeness.

Fig. 7 shows the distribution probability of the *All-pairs* outcomes; this histogram leaves a large number of blank spaces

Authorized licensed use limited to: Universidad de Zaragoza. Downloaded on December 11,2020 at 09:07:19 UTC from IEEE Xplore. Restrictions apply.

throughout the possible decimal outcomes as expected, since the bit correlation prevents $2^{N(N-1)/2} - N!$ states from being visited; however, interestingly enough the system is uniformly distributed over the remaining $N!$ values. The escalation of the entropy with the number of oscillators is shown in Fig. 1 (pink dotted line)

Since each state consists of all possible pairs that can be made out of a N oscillator matrix, any other topology construction $\mathcal{T}_0$ will have a space of states which will be a subset of the *All-pairs* space, and thus the entropy of $\mathcal{T}_0$ will be minor or equal than that of *All-pairs*. This still stands for a construction such that it extracts the maximum possible entropy from the matrix, thus implying that *All-pairs* actually deploys the maximum possible entropy, $\log_2 N!$ (see pink dotted line overlapping green line in Fig. 1).

D. k-modular topology

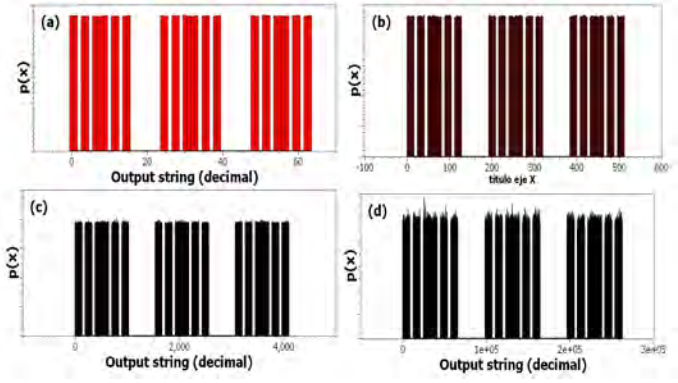

Figure 8. Probability distributions of the outcome on *3-modular* topology for different number of oscillators: *(a)* $N = 6$, (b) $N = 9$, (c) $N = 12$, (d) $N = 18$.

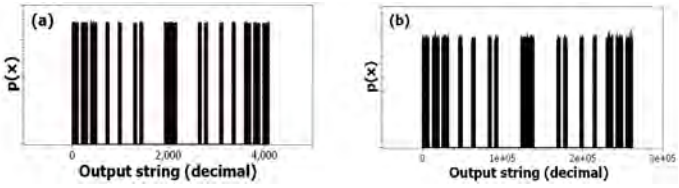

Figure 9. Probability distribution*(a)* $N = 8$, (b) $N = 12$.

The family of *k-modular* topologies, which have not been reported before to the best of our knowledge, represents an attempt to combine the benefits of avoiding repetition in oscillators comparison while keeping a high S/N ratio. In order to achieve that goal the matrix of oscillators is divided in N/k groups of k oscillators; each of this modulus is treated like an independent RO-PUF of $N = k$ oscillators, which is evaluated in an *All-pairs* fashion as to produce $k(k-1)/2$ bits. Thus the total number of bits extracted from this topology is $N(k-1)/2$ bits. Since every modulus is unconnected to the rest and entropy turns out to be an additive magnitude, the total entropy deployed by this system is expected to be:

$$S = \frac{N}{k} \times \log_2 k! \tag{4}$$

Correspondingly the entropy per bit and entropy per oscillator ratios are given by:

$$\frac{S}{\text{bit}} = 2\frac{\log_2 k!}{k\,(k-1)} \tag{5}$$

$$\frac{S}{N} = \frac{\log_2 k!}{k} \tag{6}$$

The probability distributions for the specific cases of $k = 3$ and $k = 4$ are shown in figures 8 and 9 respectively; both of these show a clear improvement in uniformity of the distribution with respect to the *N-1* topology case shown in Fig. 6. According to expression 4, entropy is expected to be linearly dependent on N (see orange and blue dotted lines in Fig. 1), while entropy per bit ratio will be constant on the number of oscillators and expected to equal $S/\text{bit} \approx 0.86$ for $k = 3$ and $S/\text{bit} \approx 0.76$ for $k = 4$ (Fig. 2), and $S/N \approx 0.86$ for $k = 3$ and $S/N \approx 1.15$ for $k = 4$ (Fig. 3).

Regarding the uniformity of the distribution, this topology promises to be more robust against a "clever search" attack as proposed against *N-1* topology. However, it is noticeable that the entropy extracted per bit is lesser than that of either *1-out-of-2* or *N-1* topologies, which suggests the existence of different vulnerabilities other than the non-uniformity of probability distribution. Nevertheless the efficiency of the system in terms of entropy per oscillator seems to improve with respect to other topologies while keeping higher S/bit than *All-pairs* comparison, which could make this digitization proposal an interesting alternative for resource-limited systems.

V. Conclusions

Throughout this work we have analyzed the outcome probability distribution of compensated measurement PUFs, of which the best known example is RO-PUF, where the output frequencies of ring oscillators pairs are compared to generate an output binary string.

The PUF instances have been simulated with an array of N uniformly distributed pseudorandom numbers as well as a topology, i.e. a "recipe" specifying the exact way in which the comparison will be carried out. A large set of ten million different PUFs realizations is generated in a sort of Monte-Carlo simulation as to ensure enough statistic about the output distribution.

The metrics used to evaluate each probability distribution were: the total entropy of the distribution, the entropy per bit and entropy per oscillator ratios. From this figures of merit we can conclude that our proposed system performs better than others in terms of entropy per bit, while retaining a high entropy per oscillator ratio. However, it is noticeable that a system performing all possible comparisons might be underestimated in PUF design practice, since it reaches a good commitment between entropy per bit and oscillator ratios despite the large correlation between some bits.

Experimental validation over physically implemented PUFs, which is necessary in order to evaluate the influence of spatial correlation regarding FPGA implementation, will be provided in the final version of this paper on the basis of RO-PUF implementation, although the results shown are of application to a wider range of PUF types.

Authorized licensed use limited to: Universidad de Zaragoza. Downloaded on December 11,2020 at 09:07:19 UTC from IEEE Xplore. Restrictions apply.

REFERENCES

[1] H. Handschuh, G. Schrijen, and P. Tuyls, "Hardware Intrinsic Security from Physically Unclonable Functions" in *Towards Hardware-Intrinsic Security*, Springer, Berlin, Heidelberg, pp. 39-53, 2010.

[2] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," in *2007 44th ACM/IEEE Design Automation Conference*, San Diego, CA, pp. 9-14, 2007.

[3] C. Herder, M. Yu, F. Koushanfar and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," in *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126-1141, Aug. 2014.

[4] U. Rührmair, J. Sölter, F, Sehnke, "On the Foundations of Physical Unclonable Functions" in *IACR Cryptology ePrint Archive*, vol. 2009, pp. 277, 2009.

[5] R. Maes, "Physically Unclonable Functions: Constructions, Properties and Applications", Ph.D. dissertation, Dept. of Electrical Engineering, K.U. Leuven, Belgium, 2012.

[6] J. D. Bekenstein, "How does the Entropy/Information Bound Work?" in *Foundations of Physics*, vol 35, pp. 1805-1823, 2005.

[7] U. Rührmair et al., "PUF Modeling Attacks on Simulated and Silicon Data," in *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1876-1891, 2013.

[8] A. Maiti and P. Schaumont, "Improved ring oscillator PUF: An FPGA-friendly secure primitive" in *Journal of cryptology*, vol. 24, no 2, pp. 375-397, 2011.

[9] B. Gassend, "Physical random functions", M.S. thesis, Dept. of Electrical Engineering and Computer Science, MIT, Massachusetts, 2003.

[10] B. Gassend et al, "Silicon physical random functions" in *Proceedings of the 9th ACM conference on Computer and communications security*. ACM, pp. 148-160, 2002.

[11] C. D. Yin and G. Qu, "LISA: Maximizing RO PUF's secret extraction," in *2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, Anaheim, CA, pp. 100-105, 2010.

[12] A. Maiti and P. Schaumont, "Improving the quality of a Physical Unclonable Function using configurable Ring Oscillators," 2009 International Conference on Field Programmable Logic and Applications, Prague, pp. 703-707, 2009.

Authorized licensed use limited to: Universidad de Zaragoza. Downloaded on December 11,2020 at 09:07:19 UTC from IEEE Xplore. Restrictions apply.