Boosting Entropy and Enhancing Reliability for Physically Unclonable Functions

Ricardo Valles-Novo, Andres Martinez-Sanchez and Wenjie Che
Klipsch School of Electrical and Computer Engineering, New Mexico State Univeristy, Las Cruces, NM 88003, USA
Email: { rivalles, amar5150, wche }@nmsu.edu

***Abstract*—Physically Unclonable Functions (PUFs) are emerging hardware security primitives that leverage random variations during chip manufacturing process to generate unique secrets. The security level of generated PUF secrets is mainly determined by its unpredictability feature which is typically evaluated using the metric of entropy bits. In this paper, we propose a novel Pairwise Distinct-Modulus (PDM) technique that significantly improves the upper bound of PUF entropy bits from the scale of $log_2(N!)$ up to $O(N^2)$. The PDM technique boosts entropy by eliminating the correlation within PUF response bits caused by element reuse in conventional pairwise comparison. We also propose a reliability-enhancing scheme to compensate the impact on reducing reliability by saving a significant portion of potential reliable response bits. Experimental results based on a published large-scale RO PUF frequency dataset validated that the proposed technique significantly boosts PUF entropy bits from the scale of $O(N \cdot log_2(N))$ up to approach the new upper bound of $O(N^2)$ with a comparable reliability, and the reliability-enhancing technique saves 4x more on the percentage of reliable response bits.**

Keywords— Physically Unclonable Functions, Boosting Entropy Bound, Correlation Elimination, Reliability Enhancing

I. INTRODUCTION

The advent of Internet-of-Things (IoTs) poses an increasing amount of security vulnerabilities which can be leveraged by adversaries to compromise the data integrity and confidentiality of connected devices. Secrets of security mechanisms such as authentication or encryption are conventionally stored within non-volatile memories (NVMs) which are vulnerable to physical attacks [1], [2]. Physically Unclonable Functions (PUFs) have been proposed as a promising secure hardware primitive for secure secret storage due to its tamper-evident feature and the capability of generating volatile secrets. PUFs leverage the random process variations during the manufacturing process of integrated circuits (ICs) to generate unique, unpredictable and reproducible secrets for individual ICs. PUFs typically work in the form of a challenge-response mechanism where a challenge is applied as input and a binary output is generated as the corresponding response, called a challenge-response pair (CRP). The secrets generated by such challenge-response mechanism are unclonable due to the uncontrollable random variations during the chip manufacturing process. The secrecy of PUF's CRPs is usually ensured by the unpredictability property which refers to the feature that adversaries are not able to predict the response to an arbitrary challenge, and such unpredictability can be further quantitatively measured by the amount of entropy bits.

Unfortunately, the concatenation of response bits generated by a given set of known challenges does not guarantee a secure secret due to the lack of independence among these CRPs. The CRPs' independence can be undermined by either: (1) a non-uniformly distributed physical layout or (2) a response generation algorithm that determines how the PUF cells are interacted to generate response bits. We call the former as spatial correlation while the latter as functional correlation [7][13]. This paper focuses on eliminating the functional correlation that exists in response bits generation algorithms of weak PUFs, and our proposed techniques are described in the context of weak PUFs, in particular RO PUFs. Please note that strong PUFs could be constructed using weak PUFs with the help of cryptographic primitives like keyed-hash functions. The proposed technique is applicable to any weak PUFs that use pairing strategies to compare soft information of entropy source.

A. Related Work

The Ring Oscillator (RO) PUF is one of the most widely investigated PUF regarding its CRPs correlations. Several works have proposed schemes to address the spatial correlations of RO PUFs [7][12] while others [6][7] have proposed different group-based coding schemes to deal with the functional correlation. It is agreed that [11] all these different schemes are optimizing the response generation process of extracting the maximum available entropy bits of $log_2(N!)$ with N RO elements. A number of works have investigated the Entropy and unpredictability of various types of PUFs. The correlations between response bits of PUFs are evaluated by Context Tree Weighting (CTW) in [16] and researchers in [8] analyzed the unpredictability and reliability of the ASIC-implementations of five different types of PUFs. The upper bounds on the min-entropy of several strong PUFs are derived in [13] to show their weakness as secure key generators. Authors in [11] demonstrated key-recovery attacks on different types of RO PUFs by manipulating their public helper data. YIN et al proposed a polynomial regression method [7] to eliminate the spatial systematic correlation within the physical layout to improve the randomness of the RO PUF. Group-based schemes were proposed in [5][6] to explore the maximum amount of independent and reliable bits out of N ROs. A comprehensive entropy and correlation analysis of the HELP PUF was studied in [17]. Recently, a spatial autocorrelation analysis was introduced in [18] to identify correlations in the responses of single-challenge PUFs, and authors in [14] proposed an entropy pump based a configurable RO PUF to improve the low-entropy keys.

B. Our Contribution

Fundamentally different from existing related works, this paper focuses on boosting the maximum extractable entropy for N PUF elements from the existing upper bound of $log_2(N!)$ up to $N(N-1)/2$ by introducing a pairwise distinct-modulus (PDM) scheme. Fig. 1 presents a high-level concept of this proposed PDM scheme on boosting PUF entropy. The nonlinearity feature of the proposed pairwise distinct-modulus (PDM) scheme eliminates the potential correlation in CRPs introduced by elements reuse in conventional pairwise scheme. This paper makes the following contributions:

- We propose a pairwise distinct-modulus (PDM) scheme that significantly improves the entropy upper-bound for the pairwise-comparison strategy from $O(N \cdot log_2(N))$ to $O(N^2)$.
- We propose a reliability enhancing technique that compensate the negative impact on reliability by identifying and saving a significant portion of potential reliable response bits that would otherwise be discarded by the thresholding technique.
- We validate the effectiveness of the proposed entropy-boosting scheme on improving the entropy and randomness statistical results with comparable reliability using a publicly available large-scale dataset of RO frequencies.

This work is supported in part by the National Science Foundation under Grant 1914635.

978-1-7281-8952-9/20/$31.00 ©2020 IEEE

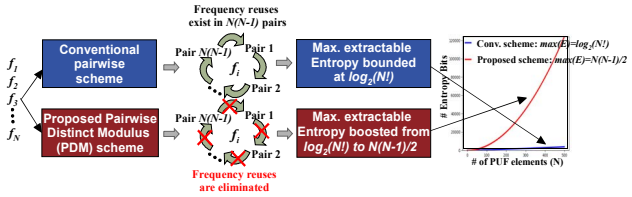

Fig. 1. Overview of the proposed entropy-boosting scheme.

- Experimental evaluations are performed to evaluate the proposed reliability-enhancing scheme using real RO PUF datasets, and results show that it improves the length of reliable response bitstring by 4x.

The rest of the paper are organized as follows. Section II introduces the relevant preliminary work. Section III describes the proposed distinct-modulus scheme in the context of RO PUFs and Section IV presents the proposed reliability-enhancing scheme. Section V presents the experimental setup and results and Section VI concludes the paper.

II. PRELIMINARIES

A. Basics of RO PUFs

The proposed distinct-modulus scheme is described in the context of RO PUFs. As shown in Fig.1, a conventional RO PUF typically consists of N identically designed Ring Oscillators that are connected to the inputs of two *N-to-1* multiplexers (MUXes). The outputs of the two MUXes are connected to two counters which are used to record the frequency values of two selected RO cells. The "Select" inputs of the two MUXes serve as the challenge which select a pair of RO cells whose frequencies are then compared to generate single response bit. A binary value '1' (or '0') is generated depending on which frequency is faster. A pairwise scheme is used to generate the response bits.

B. Entropy/Min-Entropy for PUFs Response Bits

The dependence/correlation mentioned above is detrimental to PUF's unpredictability which can be quantitively measured by the metric of Shannon entropy. Specifically, the number of independent response bits can be measured by the number of entropy and min-Entropy [19] which are computed using Equations (1) and (2) below:

$$H(X) = -\sum_{i=1}^{n} P(x_i) \cdot \log_2 P(x_i) \quad (1)$$

$$H_\infty(X) = -\log_2 \left[\max_{1\le i\le n}\left(P(x_i)\right)\right] \quad (2)$$

where X represents a discrete random variable with n possible outcomes $(x_1, x_2, \ldots x_i, \ldots x_n)$, and $P(X)$ is the probability mass function. For a binary variable X with two outcomes (0 or 1), the entropy H(X) is 1 if X is uniformly distributed, i.e., the two outcomes 0 and 1 are of equal probability (1/2) to occur.

In the RO PUF scenario, the random variable X is regarded as the K-bit response bitstring $b_1b_2\ldots b_{K-1}b_K$ generated by the $K= N(N-1)/2$ pairings for a RO PUF with N RO cells. Therefore, the variable X has $2^{(N(N-1)/2)}$ possible outcomes. If each outcome is of equal probability of $1/2^{(N(N-1)/2)}$ to occur, then the maximum entropy of K bits is achieved which indicates that each of the K response bits are fully random and independent.

III. PROPOSED DISTINCT-MODULUS SCHEME

A. Motivation of the proposed scheme

According to the pairwise scheme, the $N(N-1)/2$ response bits are not independent with each other due to the correlation. Take a group of 3 RO cells RO_1, RO_2 and RO_3 (their frequencies as f_1, f_2 and f_3) for example, there are three possible pairings for their frequencies as $P_1=(f_1, f_2)$, $P_2=(f_2, f_3)$ and $P_3=(f_1, f_3)$, and the three corresponding response bits are represented as b_{12}, b_{23} and b_{13} respectively. If $f_1 > f_2$ and $f_2 > f_3$, then it can be inferred that $f_1 > f_3$. In other words, these 3 bits $b_{12}b_{23}b_{13}$ can not be assigned values independently [5], e.g., if $b_{12} = 1$ and $b_{23} = 1$, the value of b_{13} is already determined be to 1. The dependency that exists within the $N(N-1)/2$ bits generated by the pairwise comparison can be further revealed by Table I. **All 8 possible values of 3-bit bitstring $b_{12}b_{23}b_{13}$, under all 6 possible orderings of 3 frequencies f_1, f_2 and f_3. Two values "001" and "110" will never happen, indicating dependency.** Even with $N(N-1)/2$ response bits available, the amount of independent entropy bits using the conventional pairwise scheme is upper-bounded by the number of orderings as $\log_2(N!)$, or $N\cdot\log_2(N)$ in equivalence. If each of the $N!$ orderings is of the same probability of $1/(N!)$ to occur, then the maximum entropy is obtained as $H(X) = -\sum_{i=1}^{N!}(\frac{1}{N!}\cdot\log_2\frac{1}{N!}) = \log_2 N!$ Bits

A simple "decoupled" scheme was proposed to remove the dependency by restricting using each RO cell only once but it also reduces the independent entropy bits to be $\lfloor N/2 \rfloor$. The chain-like neighbor coding scheme [12] produces $(N-1)$ response bits by only pairing neighboring and adjacent RO cells to reduce the systematic variations. An index-based syndrome (IBS) coding scheme was proposed in [4] that is information- theoretically secure. Group-based coding schemes was proposed in [5][6] to investigate the maximum amount of independent and reliable bits extractable from N Ring Oscillators..

Different from all these existing works which investigate entropy **within the upper bound of $\log_2(N!)$**, this paper focuses on boosting the entropy upper bound **beyond $\log_2(N!)$ and up to $N(N-1)/2$**, with a significant improvement from $O(N\cdot\log_2(N))$ to $O(N^2)$. This is achieved by a proposed Pairwise Distinct-Modulus (PDM) scheme to eliminate correlation in the pairings.

B. Proposed Pairwise Distinct-Modulus (PDM) scheme

The proposed response generation scheme is still a pairwise- based scheme, i.e., any two PUF elements among a group of N elements are selected to form a pair to generate a response bit, making the total number of response bits being $N(N-1)/2$ bits. However, the **vital difference** compared to the conventional pairwise comparison scheme is that a modulus operation will be applied to the soft information (digitized magnitude) of each pair of PUF elements before the comparison takes place, therefore called Pairwise Distinct Modulus (PDM) scheme. Instead of directly comparing the raw digitized magnitude (or **pre-modulus** values), we first apply a modulus operation to the pair of raw magnitude values to compute a corresponding pair of post-modulus values, and then the two post-modulus values are compared to generate a response bit. For simplicity, the raw magnitude values of each pair before and after the modulus operation are called **pre-modulus** values and **post-modulus** values, respectively.

Fig. 2(a) illustrates the proposed pairwise modulus operation with an example of a group of 3 PUF elements. With the vertical dimension representing the magnitude of the PUF elements, the raw magnitude before modulus (**pre-modulus values**) of the three PUF elements are represented by the three points as f_1, f_2 and f_3 on the left side of the figure. The arrow on top of the figure indicates a two-phase conversion process

TABLE I. ALL POSSIBLE VALUES OF 3-BIT BITSTRING B12B23B13, UNDER ALL 6 POSSIBLE ORDERINGS OF 3 FREQUENCIES F1, F2 AND F3. TWO VALUES "001" AND "110" WILL NEVER OCCUR, INDICATING DEPENDENCY.

Index	Frequency Orderings	Occur. Prob.	Response bits for each pairing		
			Pair 1 (f_1 - f_2)	Pair 2 (f_2 - f_3)	Pair 3 (f_1 - f_3)
			b_{12}	b_{23}	b_{13}
1	f1 > f2 > f3	1/6	1	1	1
2	f1 > f3 > f2	1/6	0	1	0
3	f2 > f1 > f3	1/6	1	0	0
4	f2 > f3 > f1	1/6	1	0	1
5	f3 > f1 > f2	1/6	0	0	0
6	f3 > f2 > f1	1/6	0	1	1
7	**-**	**0**	**0**	**0**	**1**
8	**-**	**0**	**1**	**1**	**0**

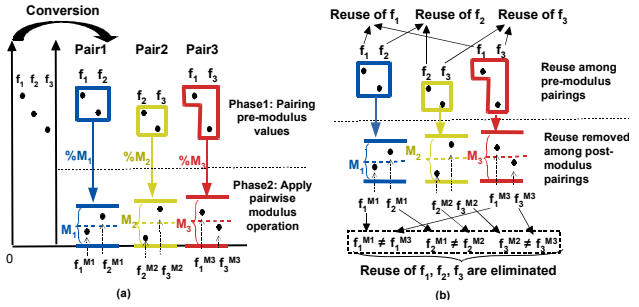

Fig. 2. Overview of the proposed pairwise distinct modulus (PDM) scheme.

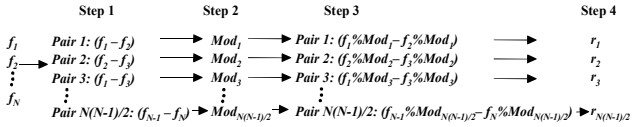

Fig. 3. Working flow of the proposed pairwise distinct-modulus scheme (PDM) for a RO PUF instance with N ROs.

where the first phase is the pairwise construction among the three elements, and the second phase applies a pairwise modulus operation to each corresponding pair of the pre-modulus values to generate the corresponding post-modulus values.

The right side of Fig. 2(a) illustrates the two phases of the conversion process: pairing pre-modulus values and applying pairwise modulus operation. The pairwise modulus operation shares a common modulus value between the two pre-modulus values within the same pair, **while distinct modulus values are used among different pairings.** This is illustrated by the three distinct modulus values M_1, M_2 and M_3 used for the three pairings in Fig. 2(a), respectively. During phase 1, the **"reuse"** scenarios of each pre-modulus value can be observed in two different pairs, e.g., f_1 is reused in Pair 1 and Pair 3 shown in the upper half of Fig. 2(b). However, such "reuse" scenario of the pre-modulus value is eliminated for the corresponding post-modulus values after phase 2, e.g., the reuse of the pre-modulus value f_1 is eliminated in its two post-modulus values f_1^{M1} and f_1^{M3} in Pair 1 and Pair 3 because of the two distinct modulus values M_1 and M_3, as shown in the lower half of Fig. 2(b). This indicates that the 'reuse' scenarios in pre-modulus pairings are 'eliminated' after the pairwise distinct modulus operation is applied. The reuse elimination is attributed to the fact that different modulus values are being used for different pairings, generating different post-modulus values that are even from a common pre-modulus value.

Fig. 3 illustrates the working flow of our proposed PDM scheme. After constructing the $N(N-1)/2$ pairings from the N frequencies (step 1 in Fig. 3), $N(N-1)/2$ distinct modulus values $M_1, \ldots, M_{N(N-1)/2}$ are used to be applied to their corresponding pairings to generate the post-modulus values which are then compared to generate the response bits (steps 2-4 in Fig. 3). The distinct modulus values $M_1, \ldots, M_{N(N-1)/2}$ can be determined by incrementally adding a step size value ΔM to its previous value, e.g., $M_i = M_1 + (\mathrm{i} - 1) \cdot \Delta M$ where $\Delta M = M_1/(N(N-1)/2)$. The first modulus value M_1 is called the "starting modulus value".

The elimination of the pre-modulus reuse scenarios using our PDM scheme is the key to reduce the correlation that exists within response bits generated among all the $N(N-1)/2$ pairings, and thus significantly improves the entropy from $O(N \cdot log_2(N))$ up to $O(N^2)$.

IV. Proposed Reliability-Enhancing Technique

In this section, we propose a pairwise offset-based technique (POT) for each post-modulus pair to enhance the reliability of the response bits generated by the proposed PDM scheme.

A. Additional noise margins for post-modulus values

In the previous section, the described pairwise distinct modulus (PDM) scheme maps each pair of pre-modulus values from a much larger magnitude into a smaller range of post-modulus values of $[0, M-1]$, where M is the applied modulus value. This mapping process can be regarded as a repetitive 'folding' operation which repeatedly subtract M at a time from the pre-modulus value until a value between $[0, M-1]$ is obtained. Although such 'folding' operation eliminates the correlation caused by the frequency reuse, it unfortunately introduces two additional response flipping boundary lines for the pair of post-modulus values. This process is illustrated in the lower half of Fig. 4(a) where a modulus value of M_1 is used and the two additional boundary lines are introduced at 0 and M_1-1 respectively for the post-modulus values f_1^{M1} and f_2^{M1}.

In the conventional thresholding technique [3], a helper data bit 1 (or 0) is generated during enrollment to record if the distance of a pair of frequencies is more (or less) than the predefined threshold distance T. Without the modulus operation, it is straightforward to apply the thresholding technique to the pre-modulus values: the inter-distance between a pair of pre-modulus values is calculated as $d_{inter}=abs(f_1-f_2)$ during enrollment and it is compared with the predefined threshold value T. The pair will be discarded if $d_{inter}<T$ and otherwise will be used later during regeneration. The inter-distance d_{inter} creates **only a single tolerance margin** for the pair of pre-modulus values, i.e., any pair with $d_{inter} > T$ will be regarded as "reliable" pair to be used for regeneration.

After applying the modulus operation of the proposed PDM scheme, however, two additional response flipping boundary lines are introduced at the two ends of the post-modulus range $[0, M_1-1]$. i.e., the low boundary line at value 0 and the upper boundary line at value (M_1-1) respectively. These two additional boundary lines are illustrated as the two blue horizontal lines in the lower half of Fig. 4(a). For any one post-modulus value that is close to any of these two boundary lines, noise fluctuation will make them 'jump' to the other end of the range $[0, Mod-1]$, flipping the relative positions of two post-modulus values and generating a response bit flip error. Therefore, two additional thresholding margins d_{lower} and d_{upper} are introduced around these two additional boundary lines as two new noise margins for a "reliable" post-modulus pair. A post-modulus pair can be regarded as a "reliable" pair only when all the three margin requirements are met at the same time, i.e., $d_{inter} > T$, $d_{lower} > T$ and $d_{upper} > T$. Such more strict requirements will significantly reduce the ratio of reliable response bits.

B. Proposed Pairwise offset technique

We propose a pairwise offset-based technique to save those "potentially reliable" pairs that are discarded as "unreliable" post-modulus pairs that meet the following two conditions: (a) meet the inter-distance threshold requirement ($d_{inter} > T$) and (b) **only meet one of the two** additional margins' requirements, i.e., either $d_{lower} > T$ and $d_{upper} < T$, or $d_{lower} < T$ and $d_{upper} > T$. These "potentially reliable" pairs are illustrated as Case2 and Case3 in Fig. 4(b), which is equivalent to meeting the requirement of $T < d_{inter} < M-2T$. The lower bound value of d_{inter} is defined as T because condition (a) needs to be met. The upper bound value of d_{inter} is $M-2T$ because the sum of d_{lower} and d_{upper} need to be no less than $2T$ given that: (i) $(d_{lower} + d_{upper}) = M - d_{inter}$ and (ii) $(d_{lower} + d_{upper}) \geq 2T$ so that a global shifting of the two post-modulus values could possibly meet both conditions of $d_{lower} > T$ and $d_{upper} > T$ simultaneously.

The flow of the proposed pairwise offset technique is described in Fig. 4(c) and it works as follows:

1) *Compute the average value of the pair of post-modulus values as* $ave = (f_1^{M1} + f_2^{M1})/2$;

2) *Compute the offset value as* $Offset = \frac{M}{2} - ave$;

3) *Add the Offset value computed in step (2) to both* f_1^{M1} *and* f_2^{M1}, *so that the new average value of the two post-modulus values is equal to M/2, i.e.,* $ave' = M/2$.

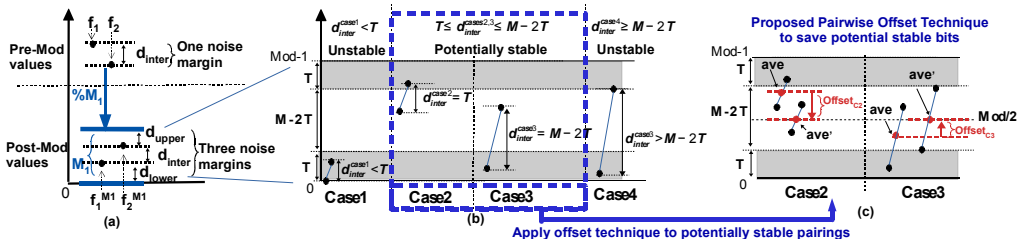

Fig. 4. (a) Added noise margins to the post-modulus values. (b) Potentially stable pairs as Case 2 and 3. (c) Proposed POT to save potentially stable pairings

It can be observed from Fig. 4(c) that after the offset operation, the two new post-modulus values will meet all the three margins' requirements to become a real "qualified reliable" pair, i.e., $d'_{inter}>T$, $d'_{lower}>T$ *and* $d'_{upper}>T$. This is also why these pairs are called "potentially reliable" pairs. The other two cases Case1 and Case 4 illustrated in Fig. 4(b) includes scenarios where any global offset operation on the two post-modulus values will not help to move the pair to be a "qualified reliable" pair. Case1 describes two post-modulus values with $d_{inter} < T$, so the first noise margin requirement will never be met no matter what offset value is applied. Case4 describes scenarios where $d_{inter} > M-2T$, which indicates that at least one post-modulus value will be located in one of the upper and lower noise margins regardless of what offset value is applied.

C. Security and overhead of the Pairwise Offset Technique (POT)

Unlike the helper data generated using the Error Correction Code (ECC) [11], the helper data of the proposed POT scheme is based on the thresholding technique which does not reveal secret information about the response bits. The range of the offset value is *[-(M/2-T/2), M/2-T/2]*, the sign and magnitude of the offset value only reveals the relative location of the **average value** of the post-modulus pair compared to *M/2*, but not any information regarding the magnitude relationship between the two post-modulus values within the pair which determines the generated response bit value. The overhead of the POT scheme depends on the number of bits used to represent the offset value whose resolution can be flexibly adjusted according to the reliability requirements.

V. Experimental Evaluation

This section validates the effectiveness of the proposed pairwise distinct modulus (PDM) scheme and the pairwise offset technique (POT) using a large scale of RO frequency dataset available in [9].

A. Experimental Setup

We used the RO counter values in the dataset provided in [9] which was collected from a set of Xilinx Artix-7 XC7A35T FPGAs. The dataset consists of two sub-datasets where the first sub-dataset was collected under room temperature and it is used for our entropy evaluation, and the second sub-dataset was collected across different temperatures and it is therefore used in our reliability evaluation. The first sub-dataset includes 217 FPGAs at 15 evaluation times under room temperature of 25°C. The second sub-dataset contains RO counter values from 50 FPGA boards across 6 different temperatures from 5°C to 55°C in steps of 10°C. For the first sub-dataset, we selected the evaluation time of 0.59 ms because it is the closest to the one used in the second sub-dataset in order to keep consistency on evaluation time in both evaluations. For simplicity, we selected the qL slice type out of 6 slice types which contains 1600 RO cells per board for both evaluations.

In order to validate that the entropy bits are in scale of *N(N-1)/2* with a group of *N* RO cells for the proposed PDM scheme, we constructed *RO* groups each of which has *N* (or #ROs_per_group) RO cells with *N = 3, 4, 5* and *6* respectively, from the dataset which contains 1600*217 = 347,200 RO cells. These constructed RO groups are used for statistical evaluation in which an ideally infinite number of experimental trials need to be performed so that the relative frequencies of occurrence of each outcome would approach agreement with the probabilities of each outcomes [10]. However, the numbers of available trials provided by the dataset is far from infinity. Specifically, a trial in our experiment refers to the process of generating a *N(N-1)/2*-bit response bitstring by all the *N(N-1)/2* pairs in a single *RO* group of *N* cells. Therefore, the limited number of available experimental trials equal to the number of available RO groups as 347,200/*N*. (Please note *#ROs_per_group=N*).

Since the number of outcomes $2^{N(N-1)/2}$ increases exponentially with *N*, the occurring frequencies of each outcome will become unacceptably low as *N* grows given the limited available trials. To address this limitation, we set an upper bound value of *N* (or *#ROs_per_group)* to be 6 to make sure that the number of trials is at least no less than the number of outcomes.

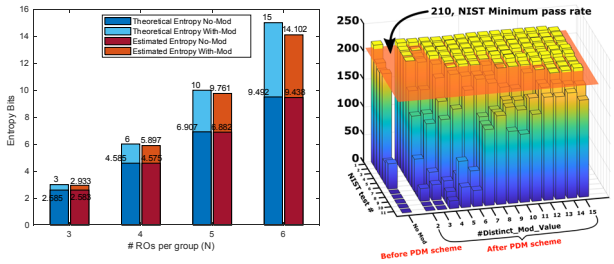

Fig. 5. (a) Theoretical and experimental entropy Comparisons between No-Mod and With-Mod schemes. (b) NIST test results.

B. Randomness Evaluation

In this section we evaluate the entropy and randomness of the proposed PDM technique. Given the fact that the entropy will vary with the magnitude of the used modulus value (discussed in Section V.C), we present our evaluation in this subsection using an optimal starting modulus value M_1 = 1800 which is obtained under the reliability restriction further discussed in the next subsection V.C.

The number of distinct modulus values (#Distinct_Mod_vals) used in our experiment can be any value between 2 and *N(N-1)/2*. If #Distinct_Mod_vals < *N(N-1)/2*, then a rotating method will be used to go back to the first distinct modulus value in a rotative way until each of the *N(N-1)/2* pairs is assigned with a modulus value.

1) Entropy and min-Entropy Evaluation

For all the values of *#ROs_per_group* being *3, 4, 5* and *6*, all available trials for each *#ROs_per_group* value were experimentally performed for two scenarios: without the PDM scheme *(No-Mod)* and with the PDM scheme *(With-Mod)*. For each listed *N* value, entropy is estimated based on Equation (1) using the probabilities calculated by the occurrence frequencies of each outcome calculated by the observed results of all trials. The experimentally estimated entropy along with the corresponding theoretical entropy upper bounds are reported in

Fig.5(a). The left blue bars for each #ROs_per_group show that the theoretical entropy limits are boosted from the scale $log_2(N!)$ to $N(N-1)/2$ by the proposed PDM scheme. This is validated by the experimental entropy results presented by the right red bars for each listed N value. It is worth noting that the estimated entropy for the *With-Mod* scheme are very close to the corresponding theoretical limits, validating our proposed claim on boosting the entropy from $O(N \cdot Log_2 N)$ to $O(N^2)$.

2) NIST Test Evaluation Results

The NIST test suit is used to evaluate the randomness of the bitstrings. In order to generate the longest possible bitstring per RO group for NIST testing, we used the maximum *#ROs_per_group* value of 6 which generates a 15-bit bitstring per RO group. With 1600 RO cells available per FPGA, $\lfloor 1600/6 \rfloor = 266$ *RO* groups are obtained per FPGA and we generate a bitstring of length *15*266=3990* bits per FPGA for NIST. The number of bitstrings is the number of FPGAs as 217. According to NIST, 11 out of 15 available tests are suitable for a bitstring length of 3990. The required minimum number of passing bitstrings is 210 with 217 bitstrings tested in total.

The NIST test results are presented in Fig. 5(b) where the passing threshold value 210 is illustrated as the orange mesh. The X-axis represents all the 11 NIST tests. From left to right, the Y-axis represents the *No-Mod* scheme as the first index followed by the *With-Mod* scheme with values of #Distinct_Mod_vals ranging from 2 to 15. For the *With-Mod* scheme, it is clearly shown that the randomness increases along with the number of #Distinct_Mod_vals, with 9 out of 11 NIST tests passed as the value of #Distinct_Mod_vals surpasses 12. The two failed tests are Approximate Entropy (NIST test #10) and Serial-Forward (NIST test #11) tests, in which 200 and 190 (close to 210) bitstrings have passed. On the other hand, Fig. 5(b) shows that only 1 out of 11 NIST tests is passed for the *No-Mod* scheme, and zero passing bitstrings is observed at half of the 11 NIST tests. These observations indicate a significant improvement in the bitstrings randomness of our proposed *With-Mod* scheme over the *No-Mod* scheme.

3) Uniqueness Evaluation on Average Inter-HD evaluation

We evaluated the uniqueness of the bitstrings generated by our proposed With-Mod (PDM) scheme using Equation (3), where m represents the total number of boards in the experiment. In our evaluation, $m = 217$. Table II reports the average inter-HD of the No-Mod scheme and our With-Mod scheme with distinct modulus values ranging from 2 to 15. The reported average inter-HD values show that the proposed With-Mod scheme significantly improves the average inter-HD from a difference of 1.1% up to 0.01% compared to the ideal value of 50%.

$$ave\_interHD = \frac{2}{m(m-1)} \sum_{u=1}^{m-1} \sum_{v=u+1}^{m} \frac{HD(R_u, R_v)}{n} \times 100\% \quad (3)$$

TABLE II. AVERAGE INTER-HD FOR NO-MOD AND WITH-MOD SCHEMES

Ave inter-HD	#ROs_per_group (N)			
	3	*4*	*5*	*6*
No-Mod	48.9766%	48.8878%	48.8336%	48.8089%
With-Mod	50.0036%	49.9929%	49.9946%	49.9973%

C. Reliability Evaluation

In this subsection, we evaluate the reliability of generated response bitstings using our proposed *With-Mod* (PDM) scheme and the proposed Pairwise Offset Technique (POT). We used a threshold value T (described in section IV.B) that equals to 25% of the applied modulus value M for each pair. The average intra-chip Hamming distance (ave-intra-HD) is used as the metric which is defined in Equation (4), where R_i is the reference response bitstring generated at room temperature, and $R'_{i,y}$ are the re-generated bitstrings from 1 up to *6* different temperature conditions available in the dataset and n is the length of generated bitstring as 15 for *#ROs_per_group=6*.

$$average\ intra\_HD = \frac{1}{6} \sum_{y=1}^{6} \frac{HD(R_i, R'_{i,y})}{n} \times 100\% \quad (4)$$

1) Optimal Modulus Value for Comparable Reliability

As discussed in section IV.A, the proposed *With-Mod* (PDM) scheme introduces two extra noise margins compared to the *No-Mod* scheme, which undermines the reliability of the bitstring. The proposed pairwise offset technique (POT) is used to enhance the corresponding reliability. In order to do a fair comparison, we define an optimal modulus value that achieves a comparable reliability of that for the *No-Mod* scheme.

Fig. 6(a) depicts the average intra-HD for the *With-Mod* scheme (both without and with the proposed POT technique applied) as a function of the magnitude of the starting modulus values (M_1) ranging from 600 to 1800 with a step of 400. The average intra-HD of 1.8012% for the *No-Mod* scheme is presented as a black horizontal solid line at the bottom of Fig. 6(a) as a comparison reference. The average intra-HD of the *With-Mod* schemes decreases as the starting modulus value (M_1) increases, with a comparable or even smaller average intra-HD value achieved when M_1 rises up to 1800. This M_1 value of 1800 is therefore used as the optimal starting modulus value in our entropy and randomness evaluation in Section V.B in order to achieve a comparable comparison with the *No-Mod* scheme. As the reliability gets improved with an increasing starting modulus value M_1, the entropy/min-Entropy decreases at a very slow rate as presented by the dashed lines in Fig. 6(a). An entropy of 14.13 is obtained at the optimal M_1 value of 1800, which is still close to the new upper entropy limit of 15.

2) Apply POT scheme to save potential reliable responses

This subsection evaluates the improved percentage of reliable bits by the proposed POT technique. Fig. 6(b) shows the average percentage of the "qualified reliable bits" over a whole bitstring length of 15 bits for both *No-Offset* and *With-Offset* schemes, respectively. For different magnitude of starting modulus values M_1, we can see that the percentage of "qualified reliable" bits for the scheme that uses the POT technique is around 31.25%, while the percentage for the scheme without the POT technique is only around 6.25%. This indicates around 4x improvement on the percentage of reliable bits of the proposed offset technique over the no-offset technique.

3) Evaluating length of Entropy bit with comparable reliability between Mod-Scheme and No-Mod

Fig. 7 evaluates the length of Entropy bits **with comparable reliability** as a function of the *#RO_per_group (or N)* of the three schemes as No-Mod scheme, With-Mod scheme without POT technique, and With-Mod scheme with POT technique, respectively. We can observe from Fig. 7 that for small *#RO_per_group* values below 21, the *No-Mod* scheme has the most entropy bits compared the other two schemes. As *#RO_per_group* increases, both With-Mod schemes surpass the No-Mod scheme and then grow at a much faster quadratic rate. The first crosspoint value is observed at *#RO_per_group=21* between the No-Mod scheme and the With-Mod Scheme with POT technique, and the second crosspoint value occurs at *#RO_per_group=201* between the No-Mod scheme and the With-Mod Scheme without POT. The large gap of the two crosspoint values indicates that the proposed pairwise offset technique significantly

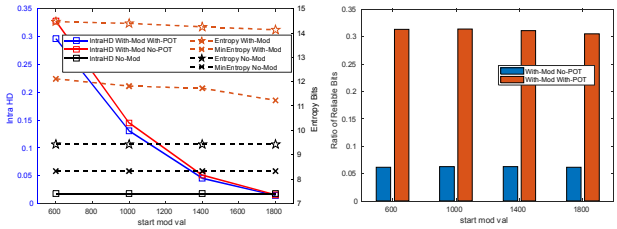

Fig. 6. (a) Explore optimal modulus magnitude to achieve comparable average Intra-HD with No-Mod Scheme. (b) Reliable bits ratio improvement of applying the proposed POT technique over no-POT technique.

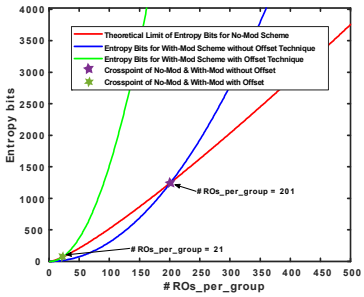

Fig. 7. Comparison of length of Entropy bits among No-Mod scheme, With-Mod scheme without POT and With-Mod scheme with POT with comparable reliability

improves the percentage of "qualified reliable" response bits. Moreover, a minimum number of 21 RO cells in a group is required to generate more entropy bits than the No-Mod scheme with a comparable reliability, and the entropy bit will grow quadratically in scale of $O(N^2)$ for *#RO_per_group>21* compared to a much slower growth rate of $O(N\log_2 N)$ for the No-Mod Scheme.

VI. Conclusion

This paper presents a pairwise distinct modulus (PDM) scheme that significantly boost PUF entropy bits from the scale of $\log_2(N!)$ up to $N(N-1)/2$ by removing the correlations within the pairwise comparison scheme. A pairwise offset technique is also proposed to compensate the reliability impact of the PDM scheme by significantly improving the ratio of qualified reliable response bits by 4x. Experimental results using a large-scale RO dataset show that the estimated entropy are approaching the new upper bound of $N(N-1)/2$ bits for the proposed PDM scheme with comparable reliability with the help of the proposed pairwise offset technique (POT). Results show the POT scheme improves the ratio of reliable bits by 4x and the two schemes can be integrated to generate entropy bits with a much faster growth rate from $O(N\log_2 N)$ to $O(N^2)$ with comparable reliability.

Acknowledgment

This work is supported in part by the National Science Foundation under Grant 1914635.

References

[1] S. H. Weingart, "Physical security devices for computer subsystems: A survey of attacks and defenses," in Proc. Cryptographic Hardware Embedded Syst (CHES)., 2000, pp. 302–317.

[2] P. Tuyls, G.-J. Schrijen, B. Skoric, J. van Geloven, N. Verhaegh, and R. Wolters, "Read-Proof Hardware from Protective Coatings," Proc. Eighth Int'l Workshop CHES '06, vol. 4249, pp. 369-383, Oct. 2006.

[3] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in Proc. ACM/IEEE Design Autom. Conf., 2007, pp. 9–14.

[4] M.-D. M. Yu and S. Devadas, ''Secure and robust error correction for physical unclonable functions,'' IEEE Design Test Comput., vol. 27, no. 1, pp. 48–65, Jan./Feb. 2010.

[5] C.E. Yin and G. Qu, "Lisa: Maximizing RO PUF's Secret Extraction," in Hardware Oriented Security and Trust (HOST), pp. 100-105, Jun. 2010.

[6] C.E. Yin, G. Qu and Q. Zhou, "Design and implementation of a groupbased RO PUF," in Design, Automation & Test in Europe, pp. 416-421, Mar. 2013.

[7] C.E. Yin and G. Qu, "Improving PUF security with regression-based distiller," in Design Automation Conference (DAC), pp. 1-6, May 2013.

[8] S. Katzenbeisser, K. Ü, V. Rožic, A.-R. Sadeghi, I. Verbauwhede and C. Wachsmann, "PUFs: Myth, Fact or Busted? A Security Evaluation of Physically Unclonable Functions (PUFs) Cast in Silicon," Cryptographic Hardware and Embedded Systems (CHES), pp. 283-301, 2012.

[9] R. Hesselbarth, F. Wilde, C. Gu, and N. Hanley, "Large scale RO PUF analysis over slice type, evaluation time and temperature on 28nm Xilinx FPGAs," in Proc. IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 126–133, 2018.

[10] Experiment (probability theory) https://en.wikipedia.org/wiki/Experiment_(probability_theory)

[11] J. Delvaux and I. Verbauwhede, "Key-recovery attacks on various RO PUF constructions via helper data manipulation," in Proc. Conf. Design Autom. Test Europe, Dresden, Germany, 2014, pp. 1–11.

[12] A. Maiti and P. Schaumont, ''Improving the quality of a physical unclonable function using configurable ring oscillators,'' in Proc. IEEE Int. Conf. Field Program. Logic Appl., Aug./Sep. 2009, pp. 703–707.

[13] J. Delvaux, D. Gu, and I. Verbauwhede, "Upper bounds on the minentropy of RO sum, arbiter, feed-forward arbiter, and S-ArbRO PUFs," in Asian Hardware-Oriented Security and Trust (AsianHOST), IEEE Asian. IEEE, 2016, pp. 1–6.

[14] Q. Wang and G. Qu, "A Silicon PUF Based Entropy Pump," IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 3, pp. 402–414, 2018.

[15] W. Liu, Y. Yu, C. Wang, Y. Cui, and M. O'Neill, "RO PUF design in FPGAs with new comparison strategies," in Proc. IEEE Int. Symp. Circuits Syst. (ISCAS), May 2015, pp. 77–80.

[16] T. Ignatenko, G. Schrijen, B. Skoric, P. Tuyls, and F. Willems, "Estimating the Secrecy-Rate of Physical Unclonable Functions with the Context-Tree Weighting Method," in IEEE International Symposium on Information Theory, Seattle, USA, July 2006, pp. 499–503.

[17] W. Che, V. K. Kajuluri, M. Martin, F. Saqib, and J. Plusquellic, "Analysis of entropy in a hardware embedded delay PUF," Cryptography, vol. 1, no. 1, Jun. 2017, Art. no. 8.

[18] F. Wilde, B. M. Gammel, and M. Pehl, "Spatial correlation analysis on physical unclonable functions," IEEE Transactions on Information Forensics and Security, vol. 13, no. 6, pp. 1468–1480, June 2018.

[19] C. E. Shannon, "A mathematical theory of communication," ACM SIGMOBILE Mobile Comput. Comm. Rev., vol. 5, no. 1, pp. 3–55, 2001.