Enlarging Reliable Pairs via Inter-Distance Offset for a PUF Entropy-Boosting Algorithm

Md Omar Faruque, Wenjie Che
Klipsch School of Electrical and Computer Engineering, New Mexico State University, Las Cruces, NM 88003, USA
Email: { faruque, wche }@nmsu.edu

2023 24th International Symposium on Quality Electronic Design (ISQED) | 979-8-3503-3475-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/ISQED57927.2023.10129308

***Abstract*—Physically Unclonable Functions (PUFs) are emerging hardware security primitives that leverage random variations during chip fabrication to generate unique secrets. The amount of random secrets that can be extracted from a limited number of physical PUF components can be measured by entropy bits. Existing strategies of pairing or grouping N RO-PUF elements have an entropy upper bound limited by $\log_2(N!)$ or $O(N \cdot \log2(N))$. A recently proposed entropy boosting technique [9] improves the entropy bits to be quadratically large at N(N-1)/2 or O(N^2), significantly improved the RO-PUF hardware utilization efficiency in generating secrets. However, the improved amount of random secrets comes at the cost of discarding a large portion of unreliable bits. In this paper, we propose an "Inter-Distance Offset (IDO)" technique that converts those unreliable pairs to be reliable by adjusting the pair inter-distance to an appropriate range. Theoretical analysis of the ratio of converted unreliable bits is provided along with experimental validations. Experimental evaluations on reliability, Entropy and reliability tradeoffs are given using real RO PUF datasets in [10]. Information leakage is analyzed and evaluated using PUF datasets to identify those offset ranges that leak no information. The proposed technique improves the portion of reliable (quadratically large) entropy bits by 20% and 100% respectively for different offset ranges. Hardware implementation on FPGAs demonstrates that the proposed technique is lightweight in implementation and runtime.**

Keywords—Physically Unclonable Functions, Reliability Enhancing, Entropy boosting

I. INTRODUCTION

It is predicted that the amount of Internet-of-Things (IoT) devices will reach 500 billion by the year 2023, becoming ubiquitous in different areas including consumer electronics, medical sensors, and industrial sectors. The rapidly growing rate of IoT devices enlarged the attacking vectors due to their ubiquitous connectivity, resource constraints, and accessibility. Secure device identification and authentication mechanisms are in great demand to ensure the trustworthiness of ubiquitously connected devices. Conventional device authentication schemes are typically built on cryptographic operations on a shared secret which requires costly non-volatile memories (NVM) for storage. Such NVM-based approach has been shown to be vulnerable to physical probing attacks [1]. Physically Unclonable Functions (PUFs) have been proposed as an alternative for device identification where the device identity can be generated upon request only when the device is powered on. Moreover, PUF-generated identity is "tamper-evident" to physical attacks because the identity derived from the underlying physical characteristic is sensitive to "invasive" tampering. Such "volatile" and "tamper-evident" features provide ideal resistance to physical attacks for secure device identification/authentication [2]. A PUF is an integrated circuit that generates secrets which are unique to each chip by leveraging the irreversible chip manufacturing variations. The subtle fabrication variability across chips is uncontrollable even by the same manufacturer, making it "unclonable" for the PUF-generated unique identifiers. PUF-generated secrets are presented in the form of "challenge-response pairs" (CRPs) where a unique response value is produced as output to a specific challenge (input).

Different PUF designs have been proposed among which Ring-Oscillator PUF (RO-PUF) has been one of the most reliable structures that fit in FPGA implementation. However, efficient secret extraction schemes have not been thoroughly explored, limiting its practicality. For example, PUF-based identification or authentication requires for a large volume of challenge-response pairs (CRPs) that are random (unpredictable). Although the pairwise strategies are able to generate a quadratically large number of N(N-1)/2 responses, there are only a small subset of $\log_2(N!)$ or O(N*log2(N)) bits that are random (unpredictable), making it vulnerable to response prediction attacks.

Pairing [3] or grouping [4][5] strategies have been proposed to interact the N RO cells to maximize the number of random and reliable response bits. However, existing RO-PUF designs with N Ring Oscillators are upper bounded to produce a maximum of $\log_2(N!)$ random entropy bits (in the scale of O(N*log2(N)). Recently a Pairwise Distinct Modulus (PDM) scheme is proposed in [6] as an entropy boosting algorithm to significantly boost the random entropy bits from $O(N \cdot \log_2(N))$ to be the quadratic $O(N^2)$, with N RO cells. The quadratically large number of $O(N^2)$ random entropy bits significantly improved the hardware utilization of RO-PUF designs, making it possible for RO-PUFs to provide a large volume of CRPs for device identification or authentications. However, a large portion of the quadratic size of responses generated by the PDM scheme is classified into unreliable bits, especially when a large threshold value is used for high reliability. This drawback reduces the number of usable reliable bits produced by the PDM scheme, making it less attractive.

In this paper, we propose an "Inter-Distance Offset (IDO)" technique that is able to convert a large portion of a Type-2 unreliable pairs in the PDM scheme to be "reliable", significantly increased the quadratically large number of usable reliable bits. The overview of the proposed IDO technique is presented in Fig.1. We make the following contributions:

- We propose an "Inter-Distance Offset (IDO)" technique that converts unreliable bits in the PDM scheme to be reliable by introducing an offset to tune the inter-distance of the unreliable pair.
- Theoretical analysis is given regarding the portion of IDO-

Authorized licensed use limited to: New Mexico State University. Downloaded on January 10,2024 at 16:09:05 UTC from IEEE Xplore. Restrictions apply.

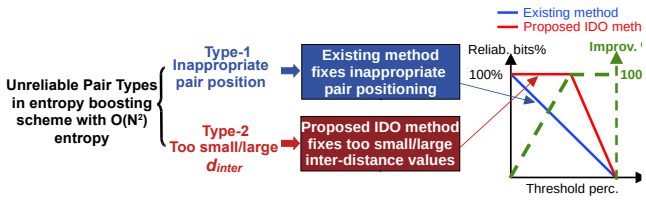

Fig. 1 Overview of the proposed Inter-Distance Offset (IDO) scheme

converted reliable bits which is further validated by experimental results using hardware PUF dataset.

- We analyze the information leakage by the public helper data (offset values) of the proposed IDO technique and identify those offset ranges that leak no information about the response as the "safe" offset range.
- We implement the proposed IDO technique on Xilinx FPGAs and demonstrated that the technique is lightweight in implementation and runtime.

The rest of the paper is organized as follows. Section II presents the related work and preliminary information. Section III gives a background review to the Pairwise Distinct Modulus (PDM) entropy-boosting scheme and the Pairwise Offset technique (POT) proposed in [9]. Section IV describes the proposed Inter-Distance Offset (IDO) scheme and Section V analyzes the theoretical percentage of IDO-converted reliable bits. Section VI gives experimental validations and evaluations on the reliability and entropy-reliability tradeoff of the IDO-converted reliable bits. Section VII analyzes the information leakage and attack resistance of the proposed IDO technique. Overhead evaluations are presented in Section VIII and Section IX concludes the paper.

II. Related Work and Preliminaries

A. Related Work

Different works have been proposed to maximize the extraction of reliable entropy bits for RO-PUFs. Authors in [3] proposed a configurable RO-PUF that enables selection of RO pairs with maximum differences to improve reliability. A longest increasing subsequence-based grouping algorithm was proposed in [4] which groups RO to generate independent and reliable responses where each group G is bounded to generate $\log_2(|G|!)$ bits. Authors in [5] improved the group-based algorithm in [4] to be more effective and suitable for error correction. A configurable RO-PUF was proposed in [6] as an entropy enhancer for low-entropy source and the trade-off between randomness and reliability was investigated. The relationship between uniqueness and entropy has been explored in [7]. A frequency offset architecture is proposed in [8] to improve the reliability of conventional RO-PUFs with a security assumption that reliable responses need to be kept secret to avoid information leakage. Other works have been proposed to reduce spatial correlations to generate more random bits [11][12] and analyzed entropy upper bounds [13]. All these works investigated reliability and entropy of RO-PUFs with an entropy bound of $\log_2(N!)$ bits from N ROs.

A recently proposed Pairwise Distinct Modulus (PDM) scheme in [9] boosted the entropy bits from $\log_2(N!)$ to the quadratically large $N(N-1)/2$, or from $O(N\cdot\log_2(N))$ to $O(N^2)$. While the entropy bits are significantly improved to be quadratically large, however, the portion of reliable bits is also reduced as the reliability threshold increases, making it less attractive. Different from existing works that investigate reliability of RO-PUFs with entropy bound of $\log_2(N!)$, this paper aims to improve the portion of reliable bits for the recently proposed PDM scheme that boosts entropy up to quadratically large $O(N^2)$ without leaking information.

B. RO PUFs and the PDM scheme [9]

The structure of a conventional RO-PUF typically consists of N identically designed Ring Oscillators whose frequency values are compared to generate response bits. An N-element RO PUF is able to generate $N(N-1)/2$ response bits using the conventional pairing scheme where, however, only $\log_2(N!)$ independent entropy bits can be generated due to the correlation caused by frequency reuse among $N(N-1)/2$ pairs. Such element reuse is eliminated by a recently proposed Pairwise Distinct Modulus (PDM) scheme [9] by applying a modulus operation to each pair using distinct modulus values (please see [9] for details), improving the entropy bits up to $N(N-1)/2$. However, the modulus operation introduces additional noise regions which classify more bits to be unreliable. This paper proposes an inter-distance offset (IDO) technique that converts a large portion of these newly introduced unreliable bits by the PDM scheme to be reliable. The portion of converted bits is quadratically large to N and hence significantly improves the usability of the quadratically large entropy bits generated by the PDM scheme.

C. Entropy and reliability of PUF response bits

PUF-based security applications rely on the randomness of PUF-generated secrets, which ensures the unpredictability feature against prediction attacks. The amount of independent and random bits that can be extracted from PUFs can be measured by entropy bits. Reliability, on the other hand, measures how re-producible the PUF-generated secrets are especially under varied external conditions. PUF-generated responses (secrets) are sensitive to changes of external conditions such as temperature or voltage due to the analog nature of PUF's physical entropy source (such as delays and resistance). Entropy and reliability resemble two sides of a coin for PUFs which typically need to be balanced to maximize usable secrets for target applications. The recently proposed PDM scheme [9] improves PUF's entropy bits to be quadratically large which significantly improves hardware utilization efficiency, however, introduces more unreliable bits.

Unlike PUF-based key generation which has nearly zero tolerance to response flip errors, PUF-based identification/ authentication has a more relaxed requirement for reliability due to some fuzzy matching methods. On the other hand, PUF-based identification/authentication protocols that directly leverage PUF responses require a large volume of challenge response pairs where CRP reuse is not allowed. The proposed Inter-distance Offset (IDO) scheme is discussed in the context of PUF-based identification/authentications in this paper.

III. Background and Overview of the Proposed Inter-Distance Offset Scheme

The proposed IDO scheme in this paper aims to improve the portion of reliable bits generated by the PDM scheme which improves the entropy bits to be quadratic. Compared to

Authorized licensed use limited to: New Mexico State University. Downloaded on January 10,2024 at 16:09:05 UTC from IEEE Xplore. Restrictions apply.

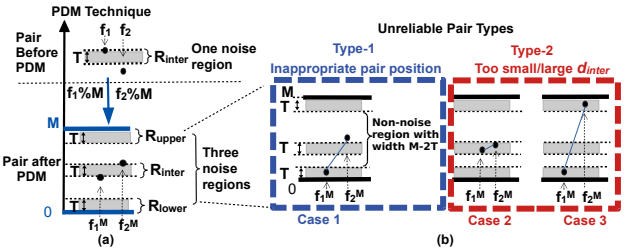

Fig. 2 (a) Three noise margins introduced by the PDM technique. (b) Two types of unreliable pairs: Type-1:Inappropriate pair position and Type-2: Extreme inter-distance values

the conventional pairwise scheme, the portion of reliable bits in the PDM scheme gets largely reduced. This reduction is due to the introduction of the two new bit-flipping boundary lines at 0 and M as the two ends of the post-modulus values after applying PDM. Fig. 2(a) describes the process of converting a pair of raw frequency (pre-modulus) values into post-modulus values by the PDM scheme. A modulus value of M is used in applying the modulus operation to the pair of raw frequency values to produce their post-modulus values which are within the new range of [0, M]. A threshold distance T is used to define the minimum distance of a reliable pair from the bit-flipping boundary lines. Before the PDM scheme, there is only one bit-flipping line which is the cross-line between the two pre-modulus values. Therefore, there is only one inter-noise region defined as the region between the pair with a distance of T. After PDM however, two new bit-flipping boundary lines are introduced at 0 and M for the post-modulus values. These two new boundaries introduce two additional noise regions "R_{lower}" and "R_{upper}" at the two edges, as shown in the left side of Fig. 2(a). A pair would be classified as unreliable if any of its data points is located within any of the three noise regions.

A. *Two Requirements and Two Types of Unreliable Pairs*

In order for a pair to be identified as reliable, it needs to meet two types of requirements: (1) the requirement for its inter-distance "d_{inter}" range, and (2) the requirement for its pair positioning.

The first requirement defines that the pair inter-distance "d_{inter}" needs to be in the range of $T< d_{inter} <M-2T$. In order to be identified as a reliable pair, both points of the pair need to be located outside of the three noise regions "R_{inter}", "R_{lower}" and "R_{upper}". Firstly, in order to make sure that both points are outside of the inter-noise region "R_{inter}", it requires that the pair inter-distance d_{inter} is larger than the width of inter-noise region, i.e., $d_{inter} > |R_{inter}| = T$. Secondly, in order to ensure that both points are located outside of the two edged noise regions "R_{lower}" and "R_{upper}", it requires that the pair inter-distance d_{inter} cannot be too large otherwise both points will be forced to be located within the noise regions "R_{lower}" and "R_{upper}" on the two edges, respectively. Here the maximum "safe" pair inter-distance d_{inter} equals to the width of the "non-noise" region (M-2T) that is in the middle between the two edged noise regions "R_{lower}" and "R_{upper}" shown in Fig. 2(b), i.e., $d_{inter} < M-2T$. The width of the "non-noise" region is calculated as the full width M minus the width of the two-edged noise regions $2T = |R_{lower}|+|R_{upper}|$. In summary, a reliable pair requires its pair inter-distance "d_{inter}" to be in the range of $T< d_{inter} <M-2T$.

Meeting this inter-distance requirement is not a sufficient condition to ensure a reliable pair. A pair also needs to be appropriately positioned, i.e., none of the two points should be positioned within the two noise regions "R_{lower}" and "R_{upper}" on the two edges. Case 1 in Fig. 2(b) gives an example where a pair that meets the first inter-distance condition ($T< d_{inter} <M-2T$) can still be an unreliable pair, because one point is inappropriately positioned within the lower noise region "R_{lower}". Therefore, the second requirement of appropriate pair position also needs to be met to ensure a reliable pair.

We classify unreliable pairs into two types depending on if the first requirement (inter-distance range) is met or not: (1) Type-1 unreliable pairs which only meet the first inter-distance requirement but not the appropriate position requirement, i.e., $T< d_{inter} <M-2T$, and (2) Type-2 unreliable pairs that even fail to meet the first inter-distance requirement, i.e., the inter-distance is either too small as $d_{inter}<T$, or too large as $d_{inter} >M-2T$. These two types of unreliable pairs are shown in Fig. 2(b).

B. *Converting Type-1 Unreliable Pairs to be Reliable Using Pairwise Offset technique [9]*

The Type-1 unreliable pairs which are inappropriately positioned can be converted into reliable pairs by a Pairwise Offset technique (POT) proposed in [9]. The POT technique shifts the whole pair towards the center so that the pair average is re-located at the center of the non-noise region at M/2, shown in Fig 3(a). This centered pair position after POT ensures the best pair position where both points are located farthest away from the noise regions R_{lower} and R_{upper} on the two edges. Since the Type-1 pair also meets the inter-distance requirement of $T< d_{inter}<M-2T$, both points after the POT are

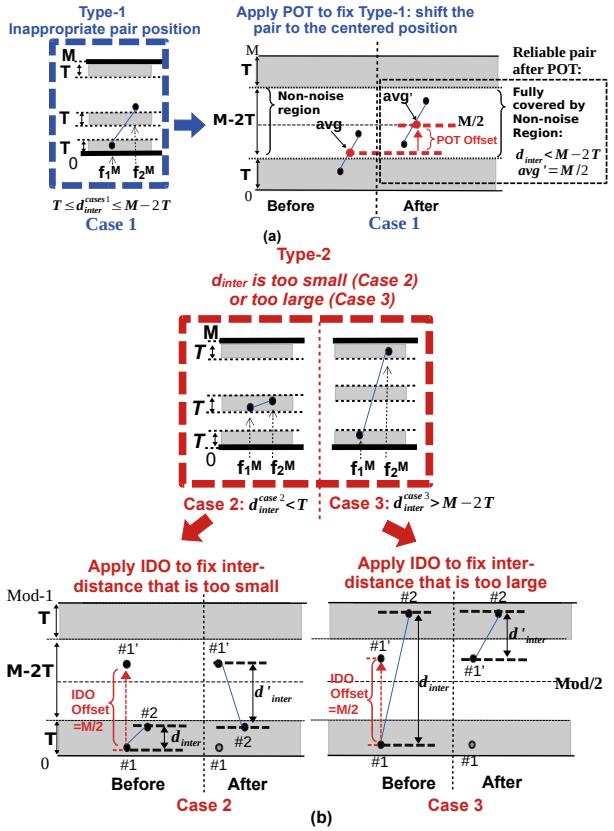

Fig. 3 (a) Type-1 unreliable pairs are addressed by the POT technique [9]. (b) Type-2 pairs addressed by the proposed IDO technique.

Authorized licensed use limited to: New Mexico State University. Downloaded on January 10,2024 at 16:09:05 UTC from IEEE Xplore. Restrictions apply.

ensured to be located within the non-noise region (with width M-2T), outside of the two edged noise regions R_{lower} and R_{upper}.

Unfortunately, the pair-centering operation of POT is not able to convert the Type-2 unreliable pairs to be reliable because the pair fails to meet the first inter-distance requirement, i.e., $d_{inter}<T$ *or* $d_{inter}>M-2T$. When $d_{inter}<T$ as is described by Case 2 in Fig.3(b), both points of the pair will always be located within the inter noise region R_{inter} (with width T) regardless of the centered pair location after POT. When $d_{inter}>M-2T$ as is depicted by Case 3, both points of the centered pair after POT will always be located outside of the non-noise region (with width M-2T) in the middle, separately located within the two-edged noise regions R_{lower} and R_{upper} respectively. Therefore, the Type-2 unreliable pairs are not able to be converted to reliable pairs because they fail to meet the inter-distance requirement of $T< d_{inter}<M-2T$.

The above analysis indicates an important observation: the condition for an unreliable pair to be converted to be reliable by POT is to meet the inter-distance range requirement, i.e., being a Type-1 pair with a moderate inter-distance range of $T< d_{inter}<M-2T$. In other words, a Type-2 unreliable pair is not able to be converted to be reliable unless it is firstly converted to a Type-1 pair with a moderate inter-distance $T<d_{inter}<M-2T$.

IV. Proposed Inter-distance Offset Scheme (IDO)

A. Proposed Inter-Distance Offset (IDO) Scheme to Convert Type-2 Pairs into Type-1 Pairs

Inspired by the above observation, we propose an Inter-distance Offset (IDO) technique that converts the Type-2 unreliable pairs into Type-1 by adjusting the pair inter-distance into the moderate range of $T<d_{inter}<M-2T$. The converted Type-1 pair can then be converted to a reliable pair by POT.

The process of applying our proposed Inter-distance offset (IDO) technique is illustrated in Fig. 3(b). The IDO technique adjusts the inter-distance by simply shifting the first data point f_1^M upwards by an appropriate amount "IDO-offset". Here, we select IDO-offset=M/2 to be the "appropriate" shifting amount which will be discussed in the next section. After the IDO-offset, the post-IDO inter-distance d'_{inter} has a large probability to be within the moderate range of $T<d'_{inter}<M-2T$. For simplicity, such a process is illustrated in the bottom left of Fig. 3(b) for the Type-2 Case 2 (where $d_{inter}<T$). In Case 2 of Fig. 3(b), the first data point f_1^M (or #1) is shifted upwards by $M/2$ to be #1', with the post-IDO inter-distance d'_{inter} increased to be larger than T, i.e., $d'_{inter}>T$ being located within the moderate range. A similar process is illustrated by the bottom right of Fig. 3(b) for Case 3 where the original inter-distance $d_{inter}>M-2T$. After applying the IDO-offset to the first data point #1, the post-IDO distance d'_{inter} is reduced to be smaller than the upper bound $M-2T$, i.e., $d'_{inter}<M-2T$. In both examples for Case 2 and Case 3, the too small inter-distance $d_{inter}<T$ and too large inter-distance $d_{inter}>M-2T$ are adjusted by the IDO-offset to be within the moderate inter-distance range of $T<d'_{inter}<M-2T$, being converted to a Type-1 pair.

B. Applying the IDO Technique and Generating Helper Data

The above-described IDO-technique is applied to a pair during the enrollment phase to generate: (1) a 2-bit helper data and (2) a "POT-after-IDO-offset" value which will be used during response regeneration to convert the Type-2 unreliable pair to be reliable. The 2-bit helper data is used to record if a pair is an IDO-converted reliable pair. It is denoted as a tuple (*helper_data_bit, IDO_offset_bit*) where the first bit "*helper_data_bit*"*=1 (or 0)* is used to indicate if a pair can be converted to be reliable (or not) by either the POT scheme or our IDO scheme. The second bit "*IDO_offset_bit*" (0 or 1) is used to indicate the type of provided offset value as POT-offset or POT-after-IDO-offset.

Specifically, the IDO flow of generating a 2-bit helper data for a pair during enrollment is described as follows:

1) *Calculate* $d_{inter} = |f^{M1}[0]-f^{M}[1]|$ *to check if the pair is Type-2 unreliable pair, i.e., Case 2 (*$d_{inter}<T$*) or Case 3 (*$d_{inter}>M-2T$*).*
2) *If Type-2, apply the IDO-offset=M/2 to shift the first raw frequency value* f_1 *for new value* $(f_1)'$*, i.e.,* $(f_1)' = f_1+M/2$.
3) *Re-calculate the new post-modulus value* $(f_1^M)' = (f_1)' \%M$ *and the new distance value* $d'_{inter} = |(f_1^M)' - f_2^M|$. *Check if the new distance is converted to Type-1 range, i.e.,* $T<d'_{inter}<M-2T$.
4) *Generate the 2-bit helper data. If converted to Type-1, record this pair as a IDO-reliable pair by specifying: (1) helper_data_bit = 1 and (2) IDO_offset_bit = 1. If not, record this pair as a pair that can not be converted to reliable by specifying: (1) helper_data_bit = 0, (2) IDO_offset_bit = 0.*
5) *Generate the POT-after-IDO-offset value if the pair is IDO reliable. The POT-after-IDO-offset* is calculated using the same process of the POT technique [9] but with the post-IDO frequency value $(f_1^M)'$*, i.e., POT-after-IDO-offset =* $M/2 - avg((f_1^M)', f_2^M)$.

The generated 2-bit helper data and the POT-after-IDO-offset will be later referred to during the response re-generation to determine if the POT-after-IDO-offset needs to be applied to convert the pair to be reliable.

C. Selection of Appropriate IDO-offset Amount

The IDO-offset value needs to be carefully selected in order to meet two conditions: (1) The IDO-offset amount attempts to maximize the probability that the post-IDO inter-distance d'_{inter} is within the moderate range, i.e., $T<d'_{inter}<M-2T$. (2) The IDO-offset value should not introduce any biased '0's and '1's into the final response bits since such bias may cause potential leakage which makes the response value more predictable. For simplicity, we use Case 2 where $d_{inter} < T$ as an example to illustrate these two conditions.

To meet the first condition, the optimal amount of the IDO-offset value is obtained when the post-IDO inter-distance d'_{inter} is located at the middle point of the moderate range between T and $M-2T$, i.e., optimal$(d'_{inter}) = T + [(M-2T) - T]/2 = M/2 -$

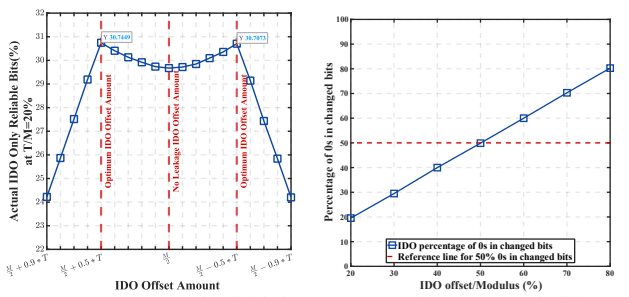

Fig. 4 (a) IDO-converted reliable bits percentage for Case 2 with different IDO-offset values. (b) Percentage of 0s among changed bits by IDO with different IDO offset value over modulus M.

Authorized licensed use limited to: New Mexico State University. Downloaded on January 10,2024 at 16:09:05 UTC from IEEE Xplore. Restrictions apply.

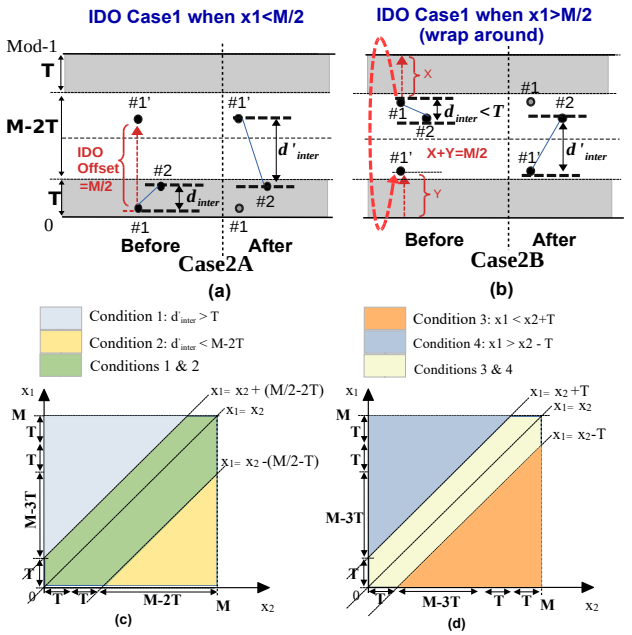

Fig. 5 IDO applied to Case 1 pairs for (a) Non-wrap-around scenario (b) wrap-around scenario. Probability illustration to meet: (c) post-IDO conditions $T< d'_{inter} < M-2T$. (d) pre-IDO condition $d_{inter} > T$.

1/2·T. Given that: (1) $IDO\text{-}offset=d'_{inter} - d_{inter}$, (2) the range of pre-IDO (x1-x2) value is -T<(x1-x2)<T, and (3) optimal(d'_{inter}) = $M/2–1/2·T$, the optimal IDO-offset amount can be determined accordingly as $IDO\text{-}offset=optimal(d'_{inter})-mean(d_{inter}) = (M/2 – 1/2·T) – 0 = M/2 – 1/2·T$. Therefore, the optimal IDO-offset amount is $(M/2 – 1/2·T)$ if only to meet the first condition that with maximum probability the post-IDO inter-distance d'_{inter} is located within the moderate range of $T<d'_{inter}<M-2T$. The above theoretic optimal IDO-offset amount of $(M/2 – 1/2·T)$ is validated using real PUF frequency data [10] as shown in Fig. 4(a). For illustration purpose we used a sample threshold value t=T/M=20%. The largest percentage of successfully converted Type-2 unreliable bits is achieved when an IDO-offset value of M/2-0.5T is used within the IDO-offset range from M/2-0.9T to M/2+0.9T.

The second condition also needs to be met which requires that the selected IDO-offset value (within the range *[0, M]*) introduces no biased '0's and '1's to the response bits, or the number of '0's and '1's in the response bits should be both equal to 50%. For illustration purpose, we take a simple scenario in Case 2 as an example where $d_{inter} < T$. The final response value after the IDO-offset will only depend on the initial position of the first point f_1^M. When the initial first point is located in the lower half, i.e., $0<f_1^M < M/2$ as shown by Case2A in Fig. 5(a), the value of first point after applying IDO-offset will be larger than the second point $(f_1^M)'=f_1^M + M/2 > f_2^M$, generating a final response bit of '1'. When the initial first point is in the upper half, i.e., $f_1^M > M/2$ as shown by Case2B in Fig.5(a), adding the IDO-offset M/2 to f_1^M will shift the first point upwards beyond the upper boundary of M and then wrap around across lower 0 boundary line moving upward, eventually located between the range of [0, M/2], or $0<(f_1^M)'<M/2$. In this scenario a final response of '0' will be generated since $(f_1^M)'<M/2 < f_2^M$. This indicates that any first point with a distance less than the IDO-offset value to the upper boundary line at *M* will be "wrapped around" to generate a response value of '0', while the remaining portion where the first point with a distance less than *(M - IDO-offset)* to the lower boundary at 0 is guaranteed to generate a response bit of '1'. In other words, the percentages of '0's and '1's are perc('0'): perc('1') = IDO-offset : (M – IDO-offset). In order to ensure 50% of '1's and '0's in the responses, it requires that IDO-offset = (M – IDO-offset) = 50%·M, or IDO-offset=1/2·M in equivalence. To summarize, an IDO-offset value of 1/2·M is needed to ensure that the second condition is met so that no biased '0's and '1's are introduced by the IDO technique. As shown in Fig.4(b), this analysis is validated using the hardware PUF data in [10]. Although the IDO-offset of M/2 is not the optimal amount that achieves the largest percentage of IDO-converted bits, the percentage is still very close to the maximum percentage as shown by the percentage value when IDO-offset=M/2 as the middle vertical line in Fig. 4(a).

V. Theoretical Analysis on Improved Percentage of Reliable Pairs

This section presents the theoretical analysis of the percentage of Type-2 pairs that can be converted to be Type-1 pairs by the IDO technique (which can be further converted to reliable pairs by POT). Note that the maximum threshold value T is obtained at M/3 when the sum width of the three noise regions $|R_{inter}| + |R_{upper}| + |R_{lower}| = 3·T = M$, occupying the whole range of [0, M]. The theoretical analysis is further validated using real PUF data published in [10].

In our theoretical analysis, we regard each of the two data points f_1^M, f_2^M as two independent random variables x1, x2 which follow a uniform distribution within the range of [0, M). Specifically, their probability density function is:

$$f_X(x) = \begin{cases} \frac{1}{M}, & if\ x \in [0, M) \\ 0, & if\ x \notin [0, M) \end{cases} \qquad (1)$$

The probability that a pair can be successfully converted to be reliable can be calculated as the probability that the two random variables meet the conditions of Type-1 pair after applying the IDO technique.

For simplicity, we use a "non-wrap-around" sub-scenario ($f_1^M <M/2$) in Case 2 ($d_{inter}<T$) of the Type-2 unreliable pairs to illustrate the analysis process, as shown in Fig. 5(a). In order to be successfully converted to a Type-1 pair, the pair needs to meet conditions at both pre-IDO phase and post-IDO phase. In the post-IDO phase, the post-IDO inter-distance d'_{inter} needs to be $T<d'_{inter}<M-2T$. In the pre-IDO phase, the pair is a Case 2 pair with $d_{inter}<T$. Given $d_{inter}=|x1–x2|$, and $d'_{inter}=|(x1+M/2)–x2|=x1+M/2-x2$, we have the following inequities:

for Post-IDO conditions:

$x1 > x2 –(M/2-T)$ condition (1)

$x1 < x2 + (M/2-2T)$ condition (2)

for Pre-IDO conditions:

$x1 < x2 +T$ condition (3)

$x1 > x2 -T$ condition (4)

Since x1 and x2 are two independent random variables with the same uniform distribution on the interval of [0, M), we can calculate the joint probability of the above conditions using a

Authorized licensed use limited to: New Mexico State University. Downloaded on January 10,2024 at 16:09:05 UTC from IEEE Xplore. Restrictions apply.

unit density plot shown in Fig. 5(c)(d). Fig. 5 (c) shows the probabilities of conditions (1) and (2) as the blue area and yellow area respectively, and the probability to meet both conditions as their overlapped area (green area). Similarly, the overlapped area (orange) in Fig. 5(d) represents the probability to meet both conditions (3) and (4). The final probability to meet all four conditions (1)-(4) equals to the overlapped area of the green area in Fig. 5(c) and the orange area in Fig. 5(d), which is determined by the lower of the two upper boundary lines x1 = x2 + (M/2-2T) and x1 = x2 +T, and the upper of the two lower boundary lines x1 = x2 + (M/2-2T) and x1 = x2 -T. After discussing the final boundary lines according to different ranges of T in [0, M/3], we obtain the final probability as the final overlapped area below:

$$P(t) = \begin{cases} \frac{1}{4} + 0.5t - 0.5 \cdot (0.5 - t)^2 - \frac{1}{8}, & when\ T < \frac{M}{6} \\ \frac{1}{8} + 0.5t - 2t^2, & when \frac{M}{6} < T < \frac{M}{4} \\ 0.5 - 1.5t, & when\ T > \frac{M}{4} \end{cases} \quad (2)$$

where t=T/M and t in [0, 1/3]. We apply the same analysis process to the other scenario of Case 2 where $f_l^M > M/2$ and Case 3, and we obtain the final probability equations below:

$$P(t) = \begin{cases} \left[\frac{1}{4} + 0.5t - 0.5 \cdot (0.5 - t)^2 - \frac{1}{8}\right] + 2t^2, & T \le \frac{M}{6} \\ \left[\frac{1}{8} + 0.5t - 2t^2\right] + \frac{1}{2}(\frac{1}{2} - t)^2, & \frac{M}{6} < T < \frac{M}{4} \\ (0.5 - 1.5t) + \frac{1}{2}t - 1.5t^2, & T \ge \frac{M}{4} \end{cases} \quad (3)$$

The theoretic probability of the IDO-converted reliable bits across $t \in [0,1/3]$ can be computed by the above equations which are graphically represented as the red curve in Fig. 6(a). It is observed that the maximum percentage of IDO-converted reliable bits of about 41.7% is obtained at T=M/6 and then the percentage gradually decreases as t increases to t=1/3.

VI. Experimental Evaluations

A. Experimental validation of theoretical percentage

To validate the theoretic probability curve using experimental PUF data, eight theoretic values (shown as light red bars in Fig. 6(a)) that are sampled from the range of $t \in [0,1/3]$ are used as reference values to be compared with the experimental data. The two *t* values that divide the range at t=1/6 (or T=M/6) and t=1/4 (or T=M/4) are also included.

The experimental percentage values are obtained by implementing our IDO-scheme using a public RO PUF dataset [10] that contains frequency values collected from 50 FPGAs under six different temperatures at 5°C, 15°C, 25°C, 35°C, 45°C and 55°C. The frequencies at room temperature of 25°C are used as the enrollment data and the data at the remaining five temperatures are used for five re-generations. The evaluated percentage of IDO-converted reliable bits is computed as the average percentage of the five (enrollment, regeneration) pairs, as shown by the dark red bars in Fig. 6(a). We can observe that the evaluated reliable bits percentage (dark red bars) closely track the corresponding theoretic probabilities (light red bars) across the range of $t \epsilon [0, 1/3]$, which validates our theoretic analysis of the percentage of IDO-converted reliable bits. Note that the evaluated values are slightly larger (about 0.7% more) than their theoretic counterparts due to a "large" base modulus value we used

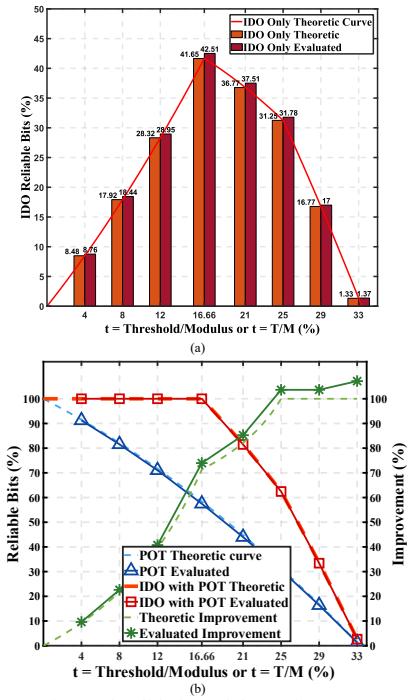

Fig. 6 (a) Experimental validation of theoretic percentage of IDO-converted reliable bits. (b) Improvement of reliable bits by IDO compared to existing POT technique [9].

M1=1800. This is because the larger the Modulus values, the less number of "folding" operations occurred during mapping a raw frequency value to a post-modulus value, resulting in a less "uniform" distribution of the post-modulus values in the range of [0, M]. This anticipation is validated by using a smaller Modulus value M1=900 and the difference between the evaluated and theoretic values become much less (less than 0.1%).

B. Analysis of improved reliable bits compared to existing POT scheme [9]

Fig. 6(b) shows the improvement in the percentage of reliable bits after applying our proposed IDO scheme (the two red curves) over the existing POT scheme (the two blue curves). It is observed that the existing POT scheme starts with the maximum percentage of 100% at t=0 and then demonstrates a constant decreasing trend as t increases to 1/3. The two red lines show the total percentage after applying our IDO scheme, where the percentage remains at the maximum 100% when $t \in [0,1/6]$, and decreases at a much slower rate than the POT-only scheme when $t \in [1/6,1/3]$. In the last range of $t \in [1/4,1/3]$, our IDO percentage demonstrates a 100% improvement over the POT-only scheme as shown by the two green lines. **To summarize**, our proposed IDO scheme improves the percentage of reliable bits to be the maximum 100% in $t \in [0,1/6]$, and improves by more than 71.5% in $t \in [1/6,1/4]$, and improves by 100% in $t \in [1/4,1/3]$.

C. Reliability of the IDO-converted reliable bits

The IDO-converted bits are generated by those "reliable pairs" that are originally converted from Type-2 unreliable pairs and further converted to reliable pairs by the POT. We evaluated the reliability of these IDO-converted "reliable bits" using the following metric:

Authorized licensed use limited to: New Mexico State University. Downloaded on January 10,2024 at 16:09:05 UTC from IEEE Xplore. Restrictions apply.

$$Reliabilitiy = 1 - avg\ intra_{HD} = 1 - \frac{1}{\#chips}\sum_{i=1}^{\#chips}\frac{1}{\#temps}\sum_{y=1}^{\#temps}\frac{HD(R_i,R'_{i,y})}{n} \times 100\% \quad (4)$$

where *avg-IntraHD* is the average intra-chip Hamming Distance that is calculated using the PUF data [10] from 50 FPGA chips (#chips=50) under the five different re-generation temperatures (#temps=5) between 5°C and 55°C with a step size of 5°C. R_i and $R'_{i,y}$ represent the response bitstrings under enrollment and the y^{th} regenerated temperature for the i^{th} chip.

The reliability of the IDO-converted "reliable" bits is related to two factors: the Modulus values and the threshold value T (or t=T/M). Fig. 7(a) illustrates the reliability of IDO-converted bits with different starting Modulus values (M1) and threshold percentage values (t=T/M). It is observed that the reliability increases as M1 increases, and a similar increasing trend is also observed as the threshold value percentage (t=T/M) increases. A reliability value as high as 99.9997% is achieved for M1=2600 at t=T/M=29%. Even higher reliability values can be achieved by increasing the t value toward 1/3 or by increasing the M1 value.

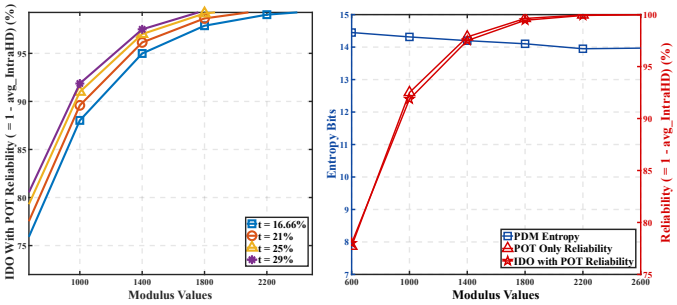

Fig. 7 (a) Reliability of the IDO scheme with the Modulus value (M1) and the threshold value T. (b) Entropy and Reliability Tradeoff

D. *Trade-off of Reliability and Entropy*

Since both Reliability and Entropy change with the magnitude of the Modulus values we use, we investigated the balance between the entropy and reliability as the starting Modulus value (M1) increases from 600 to 2200 with a step size of 400. We used *N=6* in our experiments so that we could construct enough RO instances to approximate the entropy value. The Reliability for both the POT scheme and our IDO scheme increases as the starting Modulus (M1) increases, as depicted in Fig. 7(b) by the two red lines with triangles and stars respectively. The IDO scheme has slightly lower reliability than POT but they closely track each other. On the other hand, the Entropy bits (blue line) slightly decrease as the Modulus value increases and still remains at a fairly high value around 14 out of 15 bits (here N(N-1)/2=15 with N=6) when a large modulus value of 2200 is used. The entropy value of 14 is close to the maximum 15 bits and is much higher than the $\log_2(N!)$=9.49 entropy bits bound of the existing pairwise scheme. Such a much slower decreasing rate of Entropy indicates high flexibility of our IDO scheme which enables users to trade a small amount of entropy for large reliability improvement.

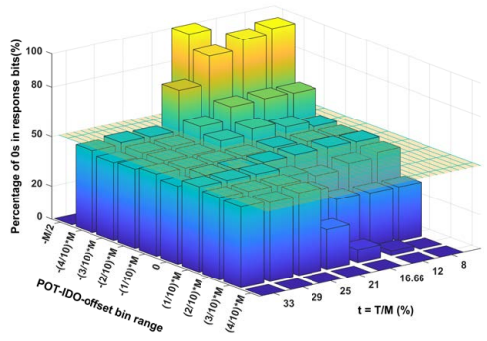

Fig. 8 Percentage of 0s in response bits in each of the 10 bin ranges of POT-after_IDO-offset with bin size of M/10

VII. Analysis of Information Leakage and Attacks

A. *Analysis of Information Leakage of Response Bits by Public Helper Data*

One aspect to assess information leakage is that if the IDO technique introduces any biased 0s or 1s to the response bits, which is discussed and addressed in Section IV.C by selecting the IDO-offset value to be M/2. A second aspect is to assess if the public helper data generated during enrollment (later used in regeneration) would leak any information about the response bit. As introduced in Section IV.B, the helper data for a pair include: (1) a 2-bit helper data and (2) an "POT-after-IDO-offset" value. The first bit "*helper_data_bit"=1 or 0* indicates if the pair can be converted to be reliable, and the second bit "*IDO_offset_bit*" (1 or 0) indicates the type of provided offset value is POT-after-IDO-offset or POT-offset. In other words, the two helper data bits would only indicate a Type-2 unreliable pair or not with inter-distance $d_{inter}<T$ or $d_{inter} >M-2T$ without revealing the response bit.

To investigate the leakage by the second piece of helper data "POT-after-IDO-offset", we evenly divided its full range of [-M/2, M/2] into 10 bins with the bin size of M/10. We then created a histogram of the percentage of 0s in the response bits in each bin range. This process is repeated for different threshold values (t=T/M) ranging from 0 to 1/3 to create a 3D histogram as shown in Fig. 8. For any particular bin range, the percentage of 0s in the response bits needs be close to 50% to demonstrate "non-biased" 0s and 1s for no leakage. As shown in Fig. 8, such "unbiased" histogram can be observed across the full bin ranges for those threshold values t that are larger than 25% (T>25%·M). When t < 25%, the percentage values start to become biased (away from 50%) for several bin ranges on the two sides towards -M/2 or M/2, while the percentage of bins in the middle still stay close to 50%.

We define a "percentage-of-0s" range of [47%, 53%] to filter out those bins that generate "biased" responses. Those IDO-converted pairs whose POT-after-IDO-offset value locate within a "unbiased" bin range are then counted as "unbiased" IDO pairs. The histogram of "unbiased" IDO pairs is presented in Fig. 9(a) where 100% IDO-pairs are "unbiased" when t> 25%, more than 70% unbiased pairs is obtained when t < 10%, and more than 30% unbiased pairs when 10%< t < 25%. These unbiased percentages are further multiplied with the total amount of IDO-converted pairs to obtain the final "unbiased" IDO-converted reliable pairs as shown in Fig. 9(b). The IDO scheme improves the percentage of "unbiased" reliable bits by about 20% on average for threshold t<25%, while improves by 100% for 25%< t < 1/3. The results show that our IDO scheme achieves the highest improvement without leakage for larger threshold values at t> 25%.

Authorized licensed use limited to: New Mexico State University. Downloaded on January 10,2024 at 16:09:05 UTC from IEEE Xplore. Restrictions apply.

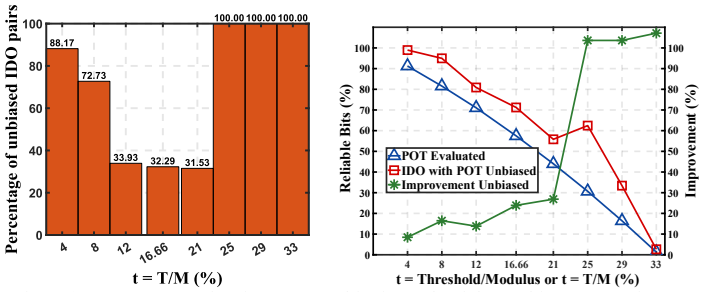

Fig. 9 (a) Percentage of 0s in response bits in each of the 10 bin ranges of POT-after-IDO-offset with bin size of M/10. (b) Improvement of reliable bits by the IDO scheme with no leakage

Please note that even the lowest 20% improvement of reliable bits of our IDO method is based on the **quadratic growing scale** of entropy bits generated by PDM as N(N-1)/2 or $O(N^2)$, which is significantly more than the $\log_2(N!)$ growing scale of existing RO-PUF designs.

VIII. Overhead Evaluation

A. Overhead of required helper data

The proposed IDO technique requires two types of helper data for each pair: (1) the offset value generated by the IDO technique during enrollment to be applied to the regenerated frequency values during response regeneration, and (2) one helper data bit which indicates if the pair is reliable or not. Since the range of the POT-after-IDO-offset value is the same as the POT-offset, i.e., [0, M/2], we can share the offset value bits between IDO and POT but with only one additional helper bit to indicate the offset type (POT-after-IDO-offset or POT-offset). Therefore, the helper data overhead of the IDO technique is only increased by one bit per response bit (to indicate the offset type) compared to the POT technique [9].

B. Implementation and Runtime Overhead

We implemented the proposed IDO technique on Xilinx Zynq7010 FPGAs and evaluated its hardware implementation overhead. Table I reports the resource utilization of the IDO technique compared to the existing Pairwise Offset Technique (POT) proposed in [9]. We can see that the number of LUTs has increased by 6.2%, the number of Carry cells has increased by 10% while the number of Flip Flops slightly drops. This indicates that the IDO technique is lightweight in implementation based on existing POT technique.

The runtime overhead for the IDO technique compared to the existing POT technique is reported in Table II. We select a larger value of N=21 (#ROs_per_group) because the tiny runtime difference for small N values (N=6) is difficult to be captured. Table II shows that to generate a total of 210 response bits, the runtime for the proposed IDO technique is slightly longer than the POT technique in [9] by 0.009 us per response bit generation.

IX. Conclusion

A recently proposed Pairwise Distinct Modulus (PDM) algorithm significantly boosts the PUF entropy bits of pairwise comparisons from $O(N\log_2 N)$ to $O(N^2)$, however, with a large portion of unreliable responses being discarded due to their too small/large pair inter-distance values. This paper proposes a lightweight Inter-distance Offset (IDO) technique that adjusts their extreme inter-distance into a moderate range which enables them to be converted to reliable pairs. The proposed IDO technique shifts one data point in the pair by an appropriate offset amount without leaking information about generated responses. The technique improves the percentage of reliable (quadratically large) entropy response bits by 20% and 100% when small and large threshold values T are used, respectively. Overhead evaluations show that the proposed scheme is lightweight in hardware implementation and runtime.

TABLE I. Implementation Overhead comparison of IDO and POT [9]

	N	# LUTs	# FFs	# Carry
POT technique in [9]	6	515	267	59
Proposed IDO method	6	547	266	65
POT technique in [9]	21	514	267	59
Proposed IDO method	21	545	266	65

TABLE II. Runtime Overhead of IDO and POT [9]

	N	# Resp	Runtime (µs)	Runtime/bit (µs)
POT technique in [9]	21	210	132	0.629
Proposed IDO scheme	21	210	134	0.638

Acknowledgment

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

References

[1] 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.

[2] 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.

[3] 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.

[4] C.E. Yin and G. Qu, "Lisa: Maximizing RO PUF's Secret Extraction," in HOST, pp. 100-105, Jun. 2010.

[5] C.E. Yin, G. Qu and Q. Zhou, "Design and implementation of a groupbased RO PUF," in DATE, pp. 416-421, Mar. 2013.

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

[7] 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.

[8] C. Gu, W. Liu, N. Hanley, R. Hesselbarth, and M. O'Neill, "A theoretical model to link uniqueness and min-entropy for PUF evaluations," IEEE Trans. Computers, 68(2):287–293, 2019.

[9] Valles-Novo, Ricardo, Andres Martinez-Sanchez, and Wenjie Che. "Boosting Entropy and Enhancing Reliability for Physically Unclonable Functions." in IEEE AsianHOST, pp. 1-6, 2020.

[10] 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 HOST, pp. 126–133, 2018.

[11] 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.

[12] F. Amsaad, A. Prasad, C. Roychaudhuri and M. Niamat, "A novel security technique to generate truly random and highly reliable reconfigurable ROPUF-based cryptographic keys," in HOST, 2016.

[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 IEEE AsianHOST, 2016, pp. 1–6.

Authorized licensed use limited to: New Mexico State University. Downloaded on January 10,2024 at 16:09:05 UTC from IEEE Xplore. Restrictions apply.