Robust RO-PUFs with Enhanced Challenge-Response Set

Giray Kömürcü
National Research Institute of Electronics and Cryptology
TÜBİTAK, 41470, Kocaeli, Turkey
Email: giray.komurcu@tubitak.gov.tr

Ali Emre Pusane, Günhan Dündar
Bogazici University, Dept. of Electrical and Electronics Eng.
34342 Bebek, Istanbul, Turkey
Email: {ali.pusane, dundar}@boun.edu.tr

***Abstract*—Ring Oscillator (RO) Physical Unclonable Functions (PUFs) are one of the best performing PUF types among various structures presented in the literature. The robustness problem of conventional RO-PUFs, that arises due to the noisy nature of ROs, is overcome with the Ordering-Based RO-PUFs presented recently. However, the shortage of usable Challenge-Response Pairs (CRPs) still limits the use of RO-PUFs, especially for authentication protocols in security systems. For a fully secure authentication based on PUF circuits, CRPs should be independent from each other and a full read-out of all CRPs should be infeasible. In conventional RO-PUFs, the number of possible CRPs is very limited and in ordering based RO-PUFs, the CRP concept is not defined at all. In this work, two methods based on RO selection is proposed for generating enhanced CRP set in ordering based RO-PUFs and their performance is analyzed in terms of area efficiency and uniqueness. With the proposed methods, robust, area and power efficient RO-PUFs with a very high number of CRPs are available for use in many security applications.**

***Keywords*-PUF, Physical Unclonable Functions, Reliability, Robustness, Ring Oscillator, FPGA, Challenge-Response, CRP**

I. Introduction

Physical unclonable functions (PUFs) have been recently developed to address security related problems. This is achieved through their main properties of uniqueness, robustness, unclonability, and unpredictability. The PUF concept was first introduced by Pappu $et\ al.$ in 2001 and offers promising and efficient solutions in IP protection, authentication, ID generation, and cryptographic key generation applications [1]. In these systems, chip specific signatures are generated uniquely on the fly; hence, the need for non-volatile memory and a secure channel to the device for ID or key storage are eliminated [2]. Another important advantage of PUFs over conventional techniques is their low cost.

Even though the first two structures proposed in the literature are Optical PUFs and Coating PUFs [1], [3], [4], their integration problems and impracticability prevented wide usage. Silicon PUFs, such as Ring Oscillator (RO) PUFs, Arbiter PUFs, SRAM PUFs, Butterfly PUFs, and Glitch PUFs dominated the area with ease of integration and low fabrication cost [5]–[10]. Silicon PUFs utilize unique intrinsic physical properties of ICs, such as threshold voltage, oxide thickness, and doping concentration to provide the basis for the characteristic properties. A PUF can also be seen as a mathematical function that maps challenges C_i to responses R_i, which can be written as $R_i \Leftarrow \text{PUF}(C_i)$, in the challenge-response pair (CRP) concept. Some PUF structures are also suitable for FPGA implementations as well.

PUF circuits can be classified as weak PUFs and strong PUFs, depending on the number of unique CRPs they can provide [8]. PUFs that supply a large set of CRPs are called strong PUFs and can be used in authentication protocols, whereas weak PUFs allow a much smaller number of challenges or does not support the CRP concept at all. SRAM PUFs support a very limited number of CRPs, since the number of SRAM cells are limited on any IC and a full read-out is possible in a short time [11]. Arbiter PUFs have the capability of generating an exponential number of CRPs based on the number of stages; hence, reading all CRPs is impossible. However, since arbiter PUFs are vulnerable to modeling attacks and are not convenient for FPGA implementation, their usage is limited [12]. RO-PUFs work reliably under changing environmental conditions and they are the most convenient PUFs for FPGA implementation [13], [14]. However, conventional RO-PUFs can be characterized by $n(\log n)$ bits of information and support a maximum number of n^2 CRPs, which also makes a full read-out possible [15].

An improved construction of RO-PUFs, the ordering based RO-PUF is a recently proposed structure with the capability of generating 100% robust, noise-free outputs. These PUFs have higher area and power efficiency than conventional RO-PUFs together with a higher entropy extraction [16], [17]. In these systems, just a single bitstream is generated, which can be used as a secret key without the need for error correction. In spite of these advantages, CRP concept is not yet defined for ordering based RO-PUFs in the literature, preventing them from being used in authentication protocols.

In Section II, we first explain the CRP properties, importance of high number of CRP availability, and possible attacks due to CRP shortage. Dynamic Programming (DP) based grouping method, which is the core of ordering based RO-PUFs is also reviewed in Section II. Next, two methods based on RO selection for constructing an enhanced CRP set in ordering based RO-PUFs are presented in Section III. Performance analysis of the proposed methods are done in Section IV. Finally, Section V concludes the paper.

II. CRP Concept in PUFs and DP Based Grouping Algorithm

In the following subsections, in order to understand the need for an enhanced CRP set and the basis for the ordering based RO-PUFs, properties and importance of the CRP concept and DP based grouping algorithm are presented in detail.

A. Properties and Importance of CRPs

Random components in the manufacturing process is the basis for PUF circuits, which enables generating chip specific outputs. One way of identifying individual circuits via PUFs is to generate a static digital output without using an input to the system. The second and more convenient way for security applications is to generate many CRPs on each IC. In this second way, the challenge is an input to the PUF circuit and the response is the output generated depending on the challenge and the transient behavior of the IC. The number of CRPs is a function of inputs to the system [18].

PUF circuits should have certain properties in terms of CRPs for a proper and secure functionality [8], [18]. Initially, evaluation of CRPs by the PUF circuit should be fast and low area consuming in order to achieve low cost and high performance. Secondly, the device should be tamper evident; hence, if an invasive attack is performed, CRP behavior should change drastically to protect the security of the system. Next, without having the particular PUF circuit at hand, predicting response R_i to a challenge C_i should be impossible. Finally, a particular CRP pair should not leak any information about a different one.

The number of CRPs that a PUF type provides increases the performance and application areas of the circuit. A high number of CRPs increases the area efficiency of the PUF circuit by allowing generation of longer and stronger PUF outputs with limited resources. Similarly, increasing the number of CRPs allows identification of bigger populations and result in a higher number of authentication processes using the same circuit, since each CRP can be used only once during authentication protocols. In addition to these, practicing an emulation attack on the device becomes impossible due to insufficient storage, when the PUF circuit supports many CRPs. Similarly, a high number of CRPs allows the users to avoid multiple usage of the CRPs and prevent the success of the man-in-the-middle attack [18], [19].

B. Dynamic Programming Based Grouping Algorithm

The main disadvantages of conventional RO-PUFs are their low entropy extraction capability and the existence erroneous outputs due to the noise present in the system. Ordering based RO-PUFs, which were introduced recently in [16], aim to overcome both of these problems. In this type of PUFs, ROs are grouped according to their frequencies, maintaining a certain amount of distance among each other, and frequency ordering of ROs within each group is used for output generation. Here, grouping ROs with frequencies that are adequately apart from each other maintains reliability. Among the two methods presented on grouping the ROs in ordering based RO-PUFs, dynamic programming (DP) seems more convenient than the longest increasing subsequence based algorithm (LISA) with its low computational complexity [17]. In the grouping step, frequencies of ROs measured at normal operating conditions and a parameter called the pre-determined frequency threshold (f_{thp}) are used. The f_{thp} parameter defines the minimum frequency difference between any two ROs in the same group, to avoid changes in ordering, due to the noise present in the system and environmental variations.

The DP method guarantees forming the largest groups with 100% robustness. With this approach, highest amount of entropy extraction from the system is achieved with minimum computational complexity [17]. The algorithm starts working on a list of RO frequencies and creates a frequency sorted list of ROs, $Fsorted[n]$. Then, each RO is linked to the nearest RO with a frequency of at least f_{thp} higher and $list[n]$ is formed. In the third step, grouping is performed to achieve maximum entropy extraction and 100% robustness. Algorithm starts from $list[1]$ and groups RO_1 with the one that $list[1]$ is pointing to, RO_j. Then, the algorithm reference point jumps to the position j and the procedure is repeated until the end of the list is reached, which completes forming the first RO group. This process is repeated until all ROs are grouped. If $list[n]$ points to an RO that is already grouped at a prior step, the nearest RO towards the end of the list is grouped instead. The algorithm outputs the list of ROs in each group, which will be used to generate the output bitstream afterwards. The pseudo code of the DP approach is presented in Algorithm 1 and explained in Example 1.

Example 1: A sample execution of the DP algorithm using 12 ROs and an f_{thp} value of 1.5 MHz is explained and illustrated in Figure 1. In the first step, 12 RO frequencies are measured and the $FreqRO[n]$ array is formed. Next, a sorted list of the RO frequencies, $Fsorted[n]$, is created. Then, a linked list, $list[n]$, is formed, which contains the information of the first available RO for grouping, for each RO in the system. In the last step, groups are formed one by one, until all ROs are grouped. Using the 12 ROs, 3 distinct groups are formed with 6, 4, and 2 ROs, respectively. The first group with 6 ROs can generate $\lfloor \log_2(6!) \rfloor$ = 9 bits of output depending on 6! = 720 possible orderings. Similarly, the second group can generate 4 bits and the last group can generate 1 bit of output. Finally, 14 bits of output is generated using 12 ROs with DP, which is significantly higher than 6 bits, the maximum number of output bits that conventional RO-PUFs can generate.

III. Enhanced CRP Set with RO Selection Methods

The only way to enhance the CRP set in ordering based RO-PUFs is to utilize inputs as challenges. For this purpose, two RO selection mechanisms are developed to use RO frequencies as challenges. The first method is to implement more ROs than the minimum required number and select a subset of these ROs prior to the DP for grouping. In the second method, a similar manner is followed, but the RO selection is performed after the grouping via the DP is completed. For both of the methods, the upper-bound of possible CRPs can be calculated as follows.

Data:
1. A linked list of ROs with their frequencies measured under normal operating conditions, $FreqRO[n]$.
2. f_{thp} for robustness
Result: Groups of ROs.
Sort $FreqRO[n]$ by frequency in increasing order: $Fsorted[n]$
for $i \leftarrow 1$ **to** $n-1$ **do**
  find the nearest element $Fsorted[j]$ that is ($Fsorted[i] < Fsorted[j]$-f_{thp}) and link i to j in $list[n]$
end
$i = 1$
while *ungrouped RO exists* **do**
  if ROi *is ungrouped* **then**
    Add ROj to the group of ROi
    Jump to $ROj(i = j)$
  end
  if ROi *is grouped* **then**
    Increment i until ROi is ungrouped
  end
  if *i=n and still ungrouped RO exists* **then**
    $i = 1$
  end
end

Algorithm 1: Dynamic programming approach in pseudo code

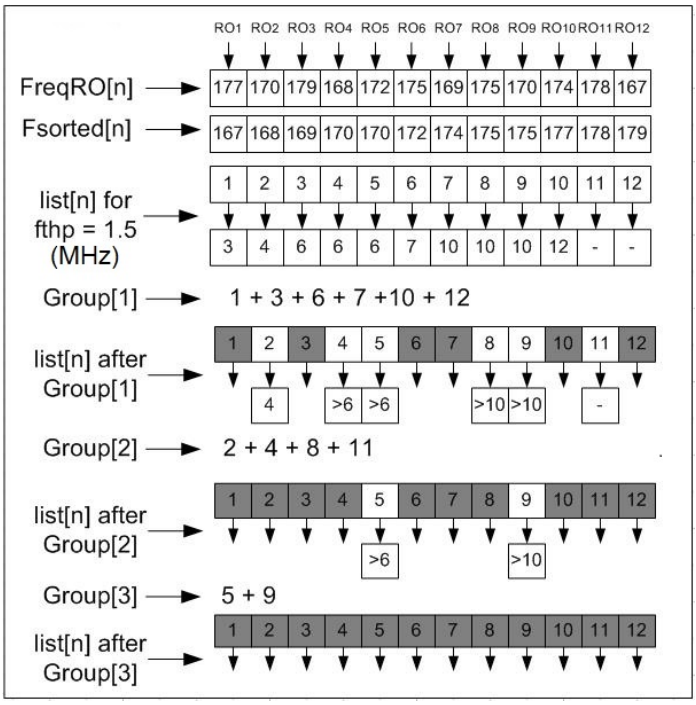

Fig. 1. DP sample execution for 12 elements.

Let RO_{imp} be the total number of implemented ROs in the PUF circuit and let RO_{min} be the minimum number of ROs required to generate a certain length of output with a particular f_{thp} value. In this case, the number of possible RO sets with RO_{min} number of ROs increases factorially with RO_{imp} and can be calculated as

$$C(RO_{imp}, RO_{min}) = \frac{RO_{imp}!}{RO_{min}!(RO_{imp} - RO_{min})!}. \quad (1)$$

Since the number of possible RO sets increases factorially, the number of CRPs that can be generated increases factorially as well. This is an important feature of the PUF circuits that has not presented for RO-PUFs previously.

For both of the methods, RO_{min} number of selected RO identities is the challenge that should be sent to the circuit during authentication and the PUF output is the response. In the first method, only the selected ROs are used as input to the DP. However, in the second method, all ROs are used for grouping and $RO_{imp} - RO_{min}$ number of ROs are deleted from the groups formed by the DP.

The main problem that may arise during the use of the proposed CRP enhancement methods is the possible closeness of the outputs. Similar outputs may be generated, if the most of the ROs selected by two challenges are the same. The solution proposed is to increase RO_{imp}, which increases the number of different RO sets. Random selection of the challenges from a large group will have a small probability of generating similar outputs. Alternatively, analyzing the CRPs prior to usage for possible similarities at the output and deleting the problematic CRPs will eliminate the risk completely.

The effectiveness of the RO selection methods is proved via repeating Example 1. For the first method, an RO set of 12 elements is created. Then, two subsets composed of 9 ROs are selected from the whole set and an f_{thp} value of 1.5 MHz is used for the DP. As seen in Figure 2, DP generates two different groupings using the two RO subsets, which generate different responses. For the second method, after the grouping is completed, two challenges are applied to the system and three ROs are deleted from the groups depending on the challenge applied, resulting in different groups; hence, different responses, as shown in Figure 3. Both examples verify the effectiveness of the proposed RO selection methods developed for enhanced CRP generation in ordering based RO-PUFs.

IV. Analysis of RO Selection Methods

Analysis of the proposed methods is performed via creating a large set of CRPs and measuring their performance depending on the uniqueness metrics developed in [20]. Previous works on the ordering based RO-PUFs indicate that, for an output length of 128 bits, 160 ROs seem enough even under extreme environmental conditions [17]. Since 128 bits is suitable for many applications, CRP generation capability of RO selection methods for each RO added to the system of 160 ROs is calculated based on the formula presented in the previous section. For this system, adding each RO increases the CRP count factorially and the total number of CRPs exceeds 10^{10}

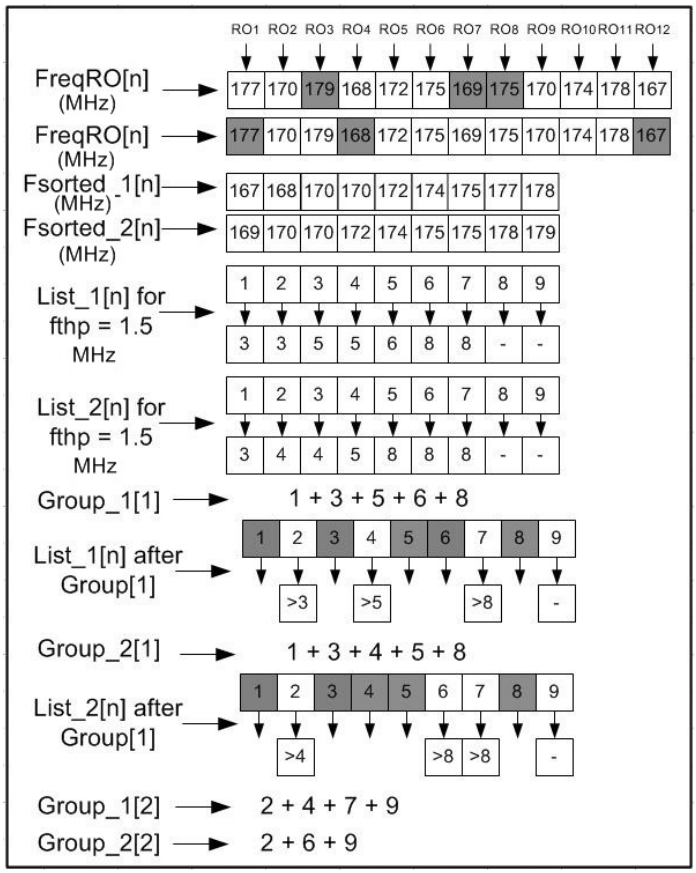

Fig. 2. DP sample execution for RO selection method before DP.

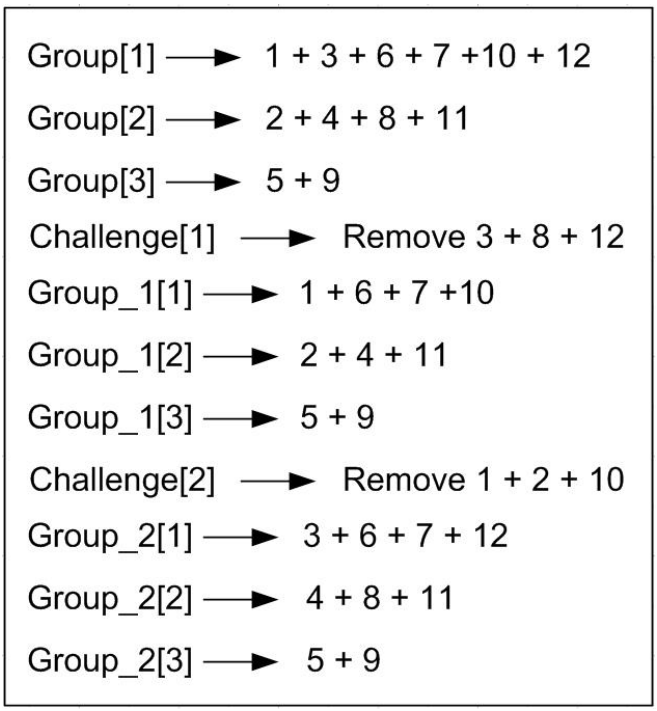

Fig. 3. DP sample execution for RO selection method after DP.

and 10^{50} for 5 and 50 additional ROs, respectively. A number of CRPs vs. additional ROs comparison is given in Figure 4.

Uniqueness analysis parameters defined in [20] are used to determine the independence of CRPs, which is the most important quality factor for the proposed CRP enhancement methods. Hamming distance (HD) of the outputs is the first quality metric, U_QM1, and can be defined as

$$U\_QM1 = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{HD(Ri, Rj)}{n}.100\%, \quad (2)$$

where n is the output bit length, k is the total number of outputs, and R_i is the ith output. U_QM1 has an ideal value of 0.5.

Closeness of the distribution of Hamming distances to a Gaussian distribution is the second quality factor. U_QM2 can be defined as

$$U\_QM2 = Corr(DIS\_HD, Gaus(Mn(HD\_PUF), \sigma)), \quad (3)$$

where DIS_HD is the distribution of HDs of the collected data, $Mn(HD\_PUF)$ and σ are the mean and standard deviation of HDs of the collected data, respectively and $Corr$ is the correlation function. If the outputs of the PUF exhibit a good distribution, U_QM2 will be closer to 1.

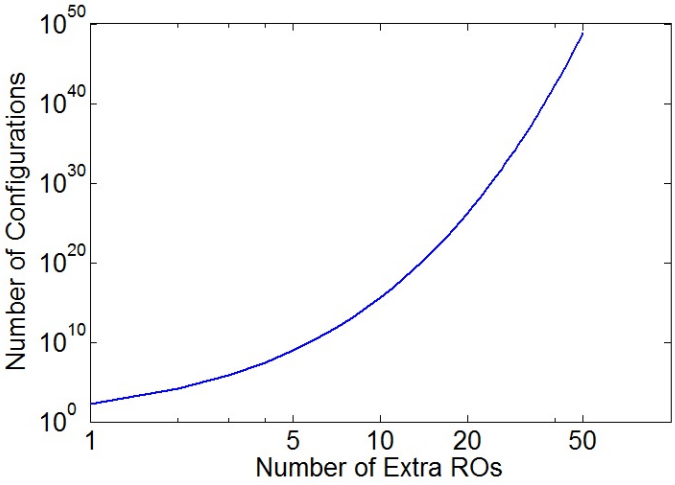

Fig. 4. Number of CRPs vs. Additional ROs

The third quality metric for uniqueness, U_QM3, determines the quality of outputs according to the Gilbert-Varshamov Bound (GVB). U_QM3 evaluates the quality of design according to the minimum HD of output pairs. A higher quality design will have a larger value for this metric.

In order to analyze the RO selection before DP method, 10 different RO sets composed of 165, 170, 175, 180, 185, 190, 195, 200, 205, and 210 ROs, whose frequencies follow the Gaussian distribution are created in MATLAB environment. Mean and standard deviation of the RO frequencies are derived from FPGA implementation measurements. Next, 10,000 subsets are created composed of 160 ROs by random selection

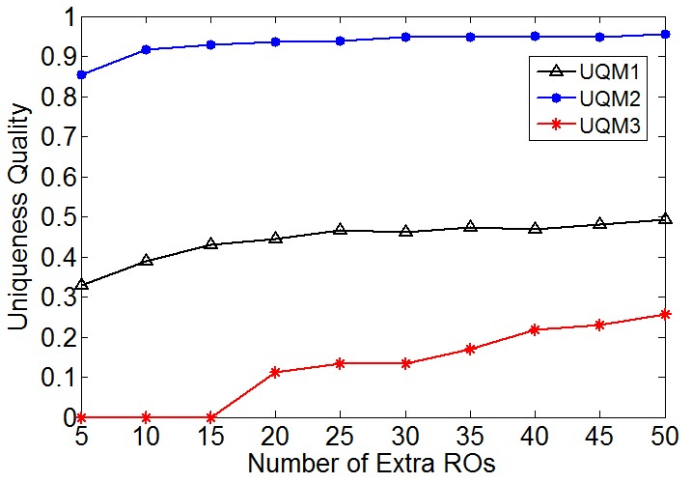

Fig. 5. Uniqueness Quality vs. Additional ROs for RO selection before DP method.

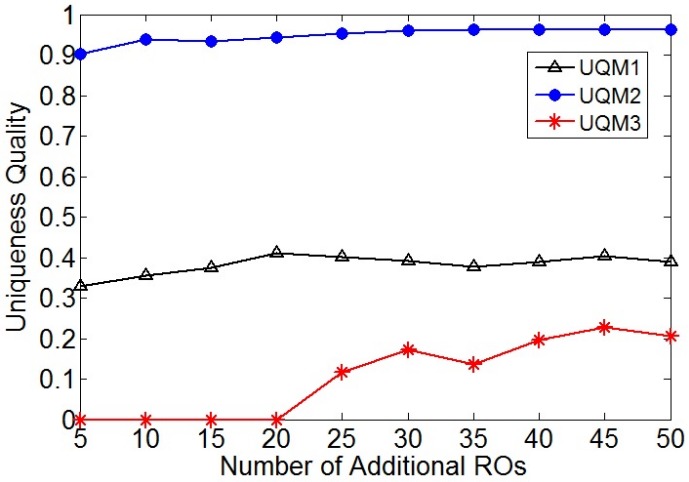

Fig. 6. Uniqueness Quality vs. Additional ROs for RO selection after DP method.

from the whole RO set. These subsets are used to generate 128 bit long outputs. Finally, for each RO set, 10,000 PUF outputs are generated for analysis.

U_QM1, U_QM2, and U_QM3 are used to analyze the uniqueness of the outputs. As seen in Figure 5, uniqueness quality increases as the number of implemented ROs increases. Adding 20 ROs to the system increases U_QM1 over 0.95 and U_QM2 over 0.45, which are close to the ideal values of 1.00 and 0.5, respectively. Also, U_QM3 indicates that adding 20 or more ROs generate unique responses to different challenges within a set of 10,000 CRPs.

RO selection after DP method is analyzed via creating 10 different RO sets composed of 165, 170, 175, 180, 185, 190, 195, 200, 205, and 210 ROs, whose frequencies follow the Gaussian distribution in MATLAB environment. In the next step, the DP algorithm is applied to the 10 sets of ROs created and the groups are formed. Then, for each RO set, ROs are deleted randomly from the groups until 160 ROs remain in the system, resulting in updated groups. For instance, 5 ROs are deleted from the groups of the RO set with 165 ROs. This is repeated for 10,000 times and 128 bit long 10,000 outputs are generated according to the updated groups for each RO set.

Again, U_QM1, U_QM2, and U_QM3 are used to analyze the uniqueness of the outputs. As seen in Figure 6, U_QM1 exceeds 0.4 when 20 or more ROs are added to the system. However, U_QM1 ceases to increase when 25 or more ROs are added and remain around 0.4. U_QM2 reaches 0.95 when 25 or more ROs are added to the system. In addition to these, U_QM3 indicates that adding 25 or more ROs generate unique responses to different challenges within a set of 10,000 CRPs.

As seen from the analysis results, both of the methods generate highly independent CRPs, when 25 or more ROs are added to the system. Both methods are convenient for security related applications, including authentication. When the results of the proposed methods are compared, U_QM1 and U_QM3 are significantly lower for the RO selection after DP method. However, U_QM2 is similar for both of the methods. The results indicate that, RO selection before DP method performs much better than the RO selection after DP method. This is due to the fact that, when the RO selection is done before DP, even a few different ROs may change the grouping significantly. However, if the RO selection is done after grouping, some groups may remain unchanged and result in degradation in the uniqueness of the results.

TABLE I
PROBABILITY OF OUTPUT COUPLES WITH HD LESS THAN THE MINIMUM HD DEFINED FOR RO SELECTION BEFORE DP METHOD

Number of ROs	Min HD ≤ 10	Min HD ≤ 20	Min HD ≤ 30	Min HD ≤ 40	Min HD ≤ 50
165	4.00E-02	1.40E-01	2.70E-01	4.11E-01	6.06E-01
170	3.80E-03	2.50E-02	8.40E-02	2.20E-01	4.80E-01
175	2.90E-04	3.70E-03	2.20E-02	9.80E-02	3.10E-01
180	8.30E-06	4.80E-04	6.80E-03	4.70E-02	2.10E-01
185	6.40E-07	4.70E-05	1.00E-03	1.20E-02	1.00E-01
190	8.00E-08	2.30E-05	8.10E-04	1.30E-02	1.27E-01
195	6.00E-08	6.60E-06	2.95E-04	6.60E-03	8.00E-02
200	0	5.00E-07	7.60E-05	4.00E-03	7.80E-02
205	0	4.40E-07	5.10E-05	2.30E-03	4.90E-02
210	0	0	7.44E-06	5.80E-04	2.30E-02

Even though the uniqueness analysis results give an important amount of information, information on the probability of output pairs that have more than a certain level of HD may be beneficial for the system design. The probability of output pairs with a HD of less than 10 to 50 bits is analyzed for the methods and presented in Table I and Table II, respectively. As expected, increasing the number of additional ROs decreases the probability of output pairs with low HD. For instance, when more than 40 additional ROs are implemented, none of the output pairs have an HD of less than or equal to 10 bits within the 10,000 outputs for both of the methods. However, if the number of implemented ROs are less than 170, almost 4% of the output pairs have less than 10 bits of HD. In addition to this, if the number of implemented ROs is more than 205, 95% of the output pairs have more than 50 bits of HD for the RO selection before DP method.

TABLE II
PROBABILITY OF OUTPUT PAIRS WITH HD LESS THAN THE MINIMUM HD DEFINED FOR RO SELECTION AFTER DP METHOD

Number of ROs	Min HD ≤ 10	Min HD ≤ 20	Min HD ≤ 30	Min HD ≤ 40	Min HD ≤ 50
165	2.50E-02	9.35E-02	2.14E-01	4.09E-01	6.60E-01
170	2.00E-03	1.80E-02	8.90E-02	2.80E-01	6.50E-01
175	2.42E-04	5.00E-03	4.10E-02	1.85E-01	5.69E-01
180	1.20E-05	5.09E-04	8.10E-03	7.10E-02	3.58E-01
185	3.22E-06	2.29E-05	5.60E-03	6.80E-02	4.19E-01
190	8.20E-07	1.20E-05	5.33E-03	9.20E-02	5.98E-01
195	1.80E-07	5.75E-06	3.90E-03	9.40E-02	6.40E-01
200	0	6.24E-06	1.13E-03	5.20E-02	5.40E-01
205	0	1.90E-06	7.60E-04	5.50E-02	5.40E-01
210	0	1.28E-06	3.97E-04	3.00E-02	4.08E-01

TABLE III
MINIMUM HD AMONG 128 BIT OUTPUTS WITHIN 10000 CRPS AND AREA OVERHEAD BASED ON THE NUMBER OF ROS

Number of ROs	Min HD among 128 bit output Before DP Method	Min HD among 128 bit output After DP Method	Area Overhead
165	0	0	0.031
170	0	0	0.063
175	0	0	0.094
180	2	0	0.125
185	6	2	0.156
190	10	5	0.188
195	11	5	0.219
200	15	13	0.250
205	18	14	0.281
210	22	16	0.313

The minimum HD within the output set is another analysis performed on the proposed methods. With this analysis, the system designer can implement the optimum number ROs according to the minimum HD requirement of the system. Results of the analysis and the area overhead of the proposed RO selection methods are presented in Table III. As seen from the table, the RO selection before DP method performs better than the RO selection after DP method. For the RO selection before DP method, minimum HD within a set of 10,000 CRPs is larger than 20 bits for 210 ROs, which increases the area cost by 31%. Even though the area cost is very low when the additional ROs are less than 20, similarities at the outputs are highly probable for both of the methods; hence, should be avoided for security related applications.

The main advantage of the proposed RO selection based methods is their capability of generating a high number of CRPs with a very reasonable area overhead. Highly independent responses are generated for a set of 10,000 responses with an area overhead of less than 15%. Another advantage of the proposed methods is their flexibility for the uniqueness quality and the number of CRPs desired.

V. CONCLUSION

Ordering based RO-PUFs are the first silicon PUF type developed that achieves 100% robustness. They are also suitable for FPGA implementation as well. However, CRP mechanism was not defined for ordering based RO-PUFs prior to this work, which is used commonly, especially in authentication protocols. Two CRP methods are developed based on RO selection that makes a high number of CRPs available with low area overhead. Uniqueness analysis of the generated responses show that the CRPs are highly independent and can be used securely even in critical applications. Ordering based RO-PUFs can be used extensively for both key generation and authentication with their robustness and CRP support.

REFERENCES

[1] R. S. Pappu, "Physical one-way functions." Ph.D. dissertation, Massachusetts Institute of Technology, Massachusetts, 2001.

[2] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Design Automation Conference (DAC)*, 2007, pp. 9–14.

[3] R. S. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 6, pp. 2026–2030, 2002.

[4] P. Tuyls, G. J. Shrijen, B. Skoric, J. V. Geloven, N. Verhaegh, and R. Walters, "Read proof hardware from protective coatings," in *18th Annual Computer Security Applications Conference (CHES)*, vol. 4249, 2006, pp. 369–383.

[5] D. Lim, J. Lee, B. Gasend, G.E.Suh, M. V. Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Transactions on VLSI Systems*, vol. 13, no. 10, pp. 1200–1205, 2005.

[6] B. Gassend, D. Clarke, M. V. Dijk, and S. Devadas, "Delay-based circuit authentication and applications," in *ACM Symposium on Applied Computing*, 2003, pp. 294–301.

[7] B. Gassend, "Physical random functions," M.S. Thesis, Massachusetts Institute of Technology, Massachusetts, 2003.

[8] J. Guajardo, S. Kumar, G. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *18th Annual Computer Security Applications Conference (CHES)*, vol. 4727, 2007, pp. 63–80.

[9] J. Guajardo, S. Kumar, R. Maes, G. Schrijen, and P. Tuyls, "Extended abstract: The butterfly PUF protecting IP on every FPGA," in *Hardware-Oriented Security and Trust (HOST)*, 2008, pp. 67–70.

[10] D. Suzuki and K. Shimizu, "The glitch PUF: A new delay-PUF architecture exploiting glitch shapes," in *Cryptographic Hardware and Embedded Systems (CHES)*, 2010, pp. 366–382.

[11] X. Wang and M. Tehranipoor, "Novel physical unclonable function with process and environmental variations," in *Design, Automation Test in Europe Conference Exhibition (DATE), 2010*, 2010, pp. 1065–1070.

[12] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *Symposium On VLSl Circuits Digest of Technical Papers*, 2004.

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

[14] C. Yin and G. Qu, "Temperature aware cooperative ring oscillator PUF," in *IEEE International Workshop on Hardware Oriented Security and Trust (HOST)*, 2009, pp. 36–42.

[15] U. Ruhrmair, J. Solter, and F. Sehnke, "On the foundations of physical unclonable functions," *Cryptology ePrint Archive*, vol. 277, 2009.

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

[17] G. Komurcu, A. E. Pusane, and G. Dundar, "Dynamic programming based grouping method for RO-PUFs," in *9th Conference on Ph. D. Research in Microelectronics and Electronics (PRIME)*, 2013, pp. 329–332.

[18] B. Gassend, D. Clarke, M. V. Dijk, S. Devadas, and D. Lim, "Identification and authentication of integrated circuits," *Concurrency and Computation: Practice and Experience*, vol. 16, no. 11, pp. 1077–1098, 2004.

[19] M. Majzoobi and F. Koushanfar, "Techniques for design and implementation of secure reconfigurable PUFs," *ACM Transactions on Reconfigurable Technology and Systems*, vol. 2, no. 1, 2009.

[20] G. Komurcu and G. Dundar, "Determining the quality metrics for PUFs and performance evaluation of two RO-PUFs," in *IEEE 10th International New Circuits and Systems Conference, (NEWCAS)*, 2012, pp. 73–76.