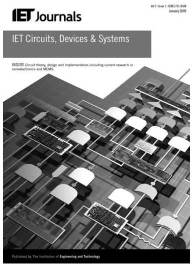
Published in IET Circuits, Devices & Systems
Received on 26th December 2013
Accepted on 13th May 2014
doi: 10.1049/iet-cds.2014.0089



ISSN 1751-858X

Enhanced challenge-response set and secure usage scenarios for ordering-based ring oscillator-physical unclonable functions

Giray Kömürcü[1], *Ali Emre Pusane*[2], *Günhan Dündar*[2]

[1]*National Research Institute of Electronics and Cryptology TÜBİTAK, 41470 Kocaeli, Turkey*
[2]*Department of Electrical and Electronics Engineering, Bogazici University, Bebek, 34342 Istanbul, Turkey*
E-mail: giray.komurcu@tubitak.gov.tr

Abstract: The number of applicable challenge–response pairs (CRPs) in physical unclonable functions (PUFs) is critical especially for authentication protocols in security systems. Ideally, full read-out of all CRPs should be infeasible and CRPs should be independent from each other for a highly secure system. CRP concept is not defined in ordering-based ring oscillator (RO) PUFs presented in the literature. In this paper, the authors propose two methods for enhanced CRP set in ordering-based RO-PUFs and analyse their performance in terms of uniqueness and area efficiency. Next, they propose three secure usage scenarios based on enhanced CRP set methods, preventing the CRPs from leaking information about each other. With the proposed systems, 100% robust, area and power efficient and secure PUF structures with exponential number of CRPs become possible that are very convenient especially for authentication protocols.

1 Introduction

Physical unclonable function (PUF) is a relatively new concept introduced by Pappu [1] in the past decade to provide efficient solutions to security related problems. Intellectual Property (IP) protection, authentication, identity (ID) generation and cryptographic key generation can be considered as the main application areas for which PUF circuits provide powerful solutions. The main advantage of PUFs over conventional techniques is their low cost and ease of integration. In addition to these, they eliminate the need for non-volatile memory (NVM) and a secure channel to the device for ID or key storage [2]. In these systems, chip specific signatures are generated uniquely on the fly. Some PUF structures are also suitable for field programmable gate array (FPGA) implementations as well [3].

Unclonability, uniqueness, robustness and unpredictability are the main features that each PUF should provide. In silicon PUFs such as ring oscillator (RO) PUFs, Arbiter PUFs, static random-access memory (SRAM) PUFs, Butterfly PUFs and Glitch PUFs [4–10], unique intrinsic physical properties of Integrated Circuits (IC), such as oxide thickness, threshold voltage and doping concentration provide the basis for the mentioned properties. In the challenge–response pair (CRP) concept, PUF is a mathematical function that maps challenges C_i to responses R_i, which can be written as $R_i \Leftarrow \mathrm{PUF}(C_i)$.

PUF types are divided into two groups as weak PUFs and strong PUFs based on the number of unique CRPs provided [7]. Strong PUFs provide a high number of CRPs based on the high amount of entropy present in the system, and thus they can be used in authentication. However, weak PUFs do not support the CRP concept or allow a small number of challenges to be applied. Arbiter PUFs support an exponential number of CRPs based on the number of stages. In such a system, reading all CRPs is impossible. However, arbiter PUFs have weaknesses allowing modelling attacks and they are not suitable for FPGA implementation, which limit their usage [11]. SRAM PUFs are not suitable for CRP applications, since the number of SRAM cells are limited on any device and full read-out is possible and very fast [12]. RO-PUFs, which are the most convenient PUFs for FPGA implementation and work reliably under changing environmental conditions, suffer from low number of CRPs [13, 14]. A conventional RO-PUF, which compares RO frequencies one-by-one, can be characterised by $n(\log n)$ bits of information and can supply a maximum number of n^2 CRPs. This makes full read-out possible [15].

Ordering-based RO-PUF is a recently developed structure that enables 100% robust, noise-free outputs [16]. Another advantage of these systems is their capability of high entropy extraction, enabling higher area and power efficiency than conventional RO-PUFs [16, 17]. In these systems, just a single output is generated, which can be used as a secret key without adding any error correction mechanism. In spite of these advantages, ordering-based RO-PUFs presented in the literature do not support authentication systems, since the CRP concept is not yet defined for them [16].

In this paper, we propose two CRP enhancement methods, titled Pre-determined Frequency Threshold Selection and RO Selection methods. Next, performance analysis and a comprehensive comparison of the proposed methods are presented in terms of CRP quality, CRP count, area, time and power efficiency. In addition to these, three different secure usage scenarios for CRP enhanced ordering-based RO-PUFs are proposed. The proposed scenarios prevent the CRPs leaking information about each other, which is mandatory for the security of PUF-based systems. With the proposed systems, 100% robust, area and power efficient and secure PUF structures with exponential number of CRPs become possible that are very convenient for many applications, such as key generation and authentication.

The rest of this paper is organised as follows. In Section 2, we first explain the CRP concept in detail, including its properties, importance of high number of CRP availability and possible attacks because of CRP shortage. Dynamic programming (DP)-based grouping method for ordering-based RO-PUFs is reviewed in Section 3. Next, enhanced CRP set with pre-determined frequency threshold selection and RO selection methods and their analysis are presented in Sections 4 and 5. Secure usage scenarios for ordering-based RO-PUFs are presented in Section 6. Finally, Section 7 concludes this paper.

2 CRP concept in PUFs

PUFs are used to generate signatures on individual ICs by utilising the random components in the manufacturing process. Generating a static digital output without using an input is the first way developed to identify circuits. The second method is to generate many CRPs on each IC, which is more convenient for many security applications. In this method, the challenge is a stimulus to the system and the response is the output that depends on the challenge and the transient behaviour of the IC. The number of CRPs is strongly related to the number of inputs to the system [18].

2.1 CRP properties

The properties of PUF circuits in terms of CRP behaviour can be stated as follows [7, 18]:

1. A response R_i to a challenge C_i should not give much information about response R_j to challenge C_j, $i \neq j$.
2. It should be almost impossible to predict response R_i to a challenge C_i without using the corresponding PUF circuit.
3. The CRP behaviour of the PUF should change drastically when an invasive attack is performed on device (tamper evidence property).
4. CRPs should be easily evaluated by the PUF circuit.

2.2 Importance of high number of CRPs

The number of CRPs that a PUF type provides is an important parameter for five reasons that are stated as follows [18, 19]:

1. Since each CRP can be used only once during authentication protocols, higher number of CRPs allow higher number of authentication processes with the same circuit.
2. High number of CRPs allows generation of longer and stronger PUF outputs with limited resources.
3. High number of CRPs allows identification of bigger populations.
4. Emulation attack, which aims at storing all possible CRPs in a memory is not applicable because of insufficient storage when the PUF circuit supports an exponential number of CRPs.
5. If CRPs are used more than once during the authentication process because of their scarcity, an attacker can make a copy of the database by a man-in-the-middle attack and unauthorised accesses to the system may become possible.

As presented above, the number of CRPs supported by the PUF circuit is very important. Adding CRP support to PUF types such as ordering-based RO-PUFs, where a single output is generated, allows the primitive to be used in a wider range of application areas. In addition to this, increasing the number of CRPs makes attacks such as emulation and man-in-the-middle impractical.

3 DP-based grouping algorithm

Since the conventional RO-PUFs do not fully extract the entropy present in the system and generate erroneous outputs up to a certain level, ordering-based RO-PUFs were introduced in [16], which provide 100% robust outputs with maximum entropy extraction. In this method, groups of ROs are formed and PUF outputs are generated according to the frequency ordering of ROs within the groups. The key point in this approach is to group ROs that are adequately apart from each other, to maintain the reliability of the system. Theoretically, the maximum number of bits generated using N ROs is up to $\lfloor \log_2(N!) \rfloor$ via ordering-based RO-PUFs [2]. In the literature, two grouping methods are proposed to group ROs. Longest increasing subsequence-based algorithm is the first method developed, and requires two measurements of each RO under extreme conditions, such as the highest and lowest operating temperatures. In addition to this, robustness problem because of the noise present in the system is eliminated via using a parameter called the frequency threshold (f_{th}) [16]. In the second method, a more efficient grouping algorithm based on DP is employed and a more conservative f_{th} value is determined (called pre-determined frequency threshold, f_{thp}) and used to overcome the complexity of measuring ROs at two extreme conditions [17]. The f_{thp} parameter in DP basically determines the minimum frequency distance of ROs within the groups, and aims to prevent changes in ordering to maintain the system reliability.

Grouping problem in ordering-based RO-PUFs is solved with 100% reliability by employing DP [17]. DP achieves extracting the maximum entropy from the system by forming the largest possible RO groups with minimum computational complexity. Using the f_{thp} parameter and the RO frequencies measured under nominal operating conditions, a list of ROs in each group is formed. Then, the output bit stream is generated using the frequency ordering of ROs in these groups.

DP algorithm starts by forming a sorted list of ROs, Fsorted [n], depending on their frequencies. Second, a linked list, list [n], is formed that points to the nearest RO with a frequency of at least f_{thp} higher, for each RO implemented in the system. Then, the grouping starts with grouping RO_1 with RO_j, which is the one that list[1] points to. Next, the RO that the list[j] points to is added to the group and the procedure lasts until the last position in the linked list is reached. At this point, forming the first group is completed. The grouped ROs are marked and the procedure is repeated until all ROs are grouped. If the linked list points to an RO that is marked as grouped, the nearest unmarked RO towards the end of list is

doi: 10.1049/iet-cds.2014.0089

```
Data:
1. A linked list of ROs with their frequencies measured under nominal 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
```

Fig. 1 *DP approach in pseudo code*

added to the particular group. The DP method is explained in Example 1 and its pseudo code is given in Fig. 1.

Example 1: In the first step, 12 RO frequencies are measured and placed into an array, *F*reqRO[*n*]. Second, a sorted list of RO frequencies, *F*sorted[*n*] is generated. In the third step, using an f_{thp} value of 1.5 MHz, list[*n*] is formed. Next, using the information kept in list[*n*], groups are formed one-by-one until all ROs are added to a group. As seen from Fig. 2, when the algorithm is applied, three distinct groups that will work reliably and extract maximum entropy from the available resources are formed. The first group with six ROs can generate $6! = 720$ possible orderings and $\lfloor \log_2(6!) \rfloor = 9$ bits. The second group with four ROs can generate 24 possible orderings resulting in 4 bits. The third group with two ROs can generate a single bit. As a result, 14 bits of output can be generated using 12 ROs in such a system.

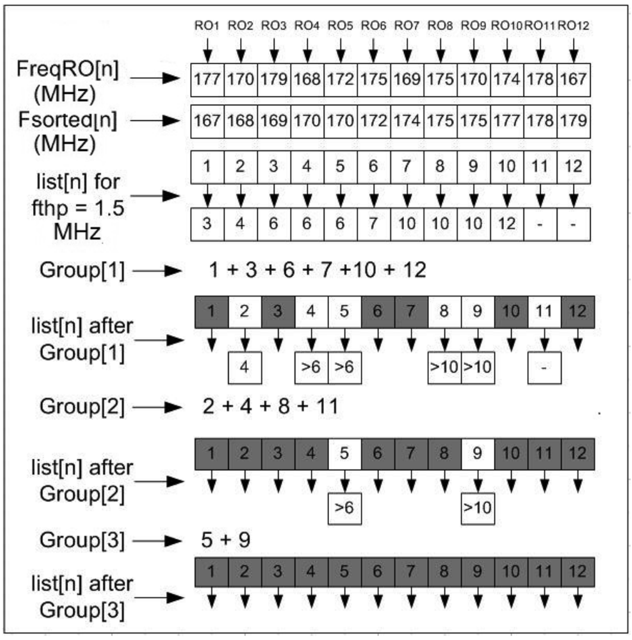


Fig. 2 *DP sample execution for 12 elements*

Enhancing the CRP set in ordering-based RO-PUFs can be achieved via utilising the inputs as challenges. As discussed previously in this section, the DP-based grouping algorithm has two sets of inputs. The first input is the list of RO frequencies measured on IC and the second input is the chosen f_{thp} value. Two methods utilising these inputs as challenges are presented in the following two sections.

4 Enhanced CRP set with f_{thp} selection method

f_{thp} is the main parameter in determining the RO groups via DP. Since outputs are created by frequency comparison within these groups, different sets of groups will result in different outputs. In this context, f_{thp} itself can be used as the challenge to the system and the PUF output will behave as the response.

The main problem in this so-called f_{thp} selection method is to determine the range of f_{thp} values and the minimum difference between any two f_{thp} values that will be used as challenges. The minimum f_{thp} value, f_{thpmin}, depends on the noise present in the system and the frequency fluctuations of ROs because of environmental variations, as described in [17]. The maximum f_{thp} value, f_{thpmax}, depends on the number of CRPs required by the application and the area, speed and power consumption requirements of the system. As the f_{thpmax} value increases, the range for selecting f_{thp} values to be used as challenges gets bigger; hence, the number of CRPs provided by the PUF circuit increases. However, increasing the f_{thpmax} value decreases the efficiencies of area, speed and power of the system. With higher f_{thp} values, ROs will form smaller groups and the entropy extraction of the system will be lower. This will increase the minimum number of ROs that will be implemented in the system in order to generate the required length of output. Increasing the number of ROs also increases the evaluation time of the PUF output and the power consumption of the system. The relation between the f_{thpmin}, f_{thpmax} and f_{thpdif} values is illustrated in Fig. 3.

f_{thpdif} value is the minimum frequency difference allowed between any two f_{thp} values. f_{thpdif} value directly determines the number of CRPs provided by the system and the

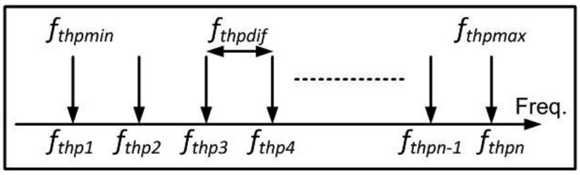

f_{thpmin}
f_{thpdif}
f_{thpmax}
Freq.
f_{thp1} f_{thp2} f_{thp3} f_{thp4} f_{thpn-1} f_{thpn}

Fig. 3 *Relation between the f_{thpmin}, f_{thpmax} and f_{thpdif} values*

independence of the outputs. When the f_{thpdif} value is small, adjacent f_{thp} values will be near each other and more CRPs will be available within the defined range. However, the formed RO groups may be similar for certain challenges, increasing the correlation of the outputs, which is a disadvantage. As the f_{thpdif} increases, the number of CRPs will diminish, but the independence of the outputs will be maintained. Since the frequency distribution of the implemented ROs in the system depends on the technology used, design and layout of the ROs, and environmental properties, the optimum value for f_{thpdif} should be determined by measuring a subset of the ICs manufactured or FPGAs programmed. The number of CRPs generated with the f_{thp} selection method, CRP_{num}, can be calculated as

$$\text{CRP}_{\text{num}} = \frac{f_{\text{thpmax}} - f_{\text{thpmin}}}{f_{\text{thpdif}}} + 1 \qquad (1)$$

To verify the effectiveness of the f_{thp} selection method, Example 1 given in Section 3 is repeated by choosing a different f_{thp} value. As shown in Fig. 4, the same RO set is grouped with an f_{thp} value of 2.5 MHz instead of 1.5 MHz using DP. As expected, the formed group contents changes drastically when the f_{thp} value is modified. This verifies the effectiveness of the f_{thp} selection method for enhancing the CRP set in ordering-based RO-PUFs.

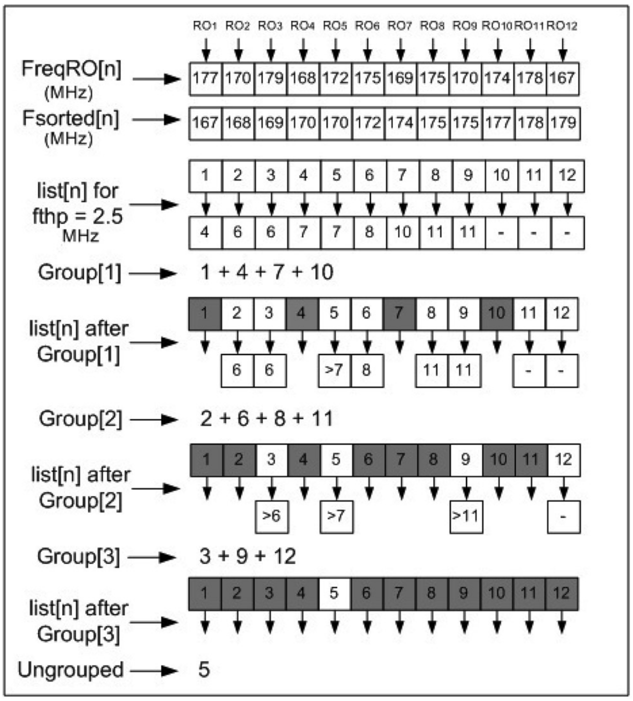


Fig. 4 *DP sample execution for 12 elements with an f_{thp} value of 2.5 MHz*

Analysis of the f_{thp} selection method is done by creating three random sets of ROs in MATLAB environment. For this purpose, 160 RO frequencies with Gaussian distribution are generated for three different RO structures with 5-, 11- and 21-stage ROs. The mean frequency and the standard deviation of the three distributions are derived based on real data measured from FPGA implementations. Then, DP algorithm is applied to each set of 160 ROs using various f_{thp} values based on the previously determined f_{thpmin}, f_{thpmax} and f_{thpdif} parameters. In this analysis, the f_{thpmin} value is set to 1 MHz for the five-stage RO structure, which seems to be an ideal value according to the measurements presented in [17], 400 and 200 kHz are chosen for the 11- and 21-stage structures, respectively. f_{thpmax} parameter is selected as 2, 1.4 and 1.2 MHz for the 5-, 11- and 21-stage ROs, respectively, which provides a range of 1 MHz for possible f_{thp} values without increasing the area consumption drastically. To determine the optimum value for the f_{thpdif} parameter, the analysis is repeated for five different f_{thpdif} values, 10, 25, 50, 100 and 200 kHz. Starting from the f_{thpmin} value, PUF outputs are generated with DP for each possible f_{thp} value that is f_{thpdif} apart from each other, until the f_{thpmax} value is reached. For instance, 101 outputs are generated for an f_{thpdif} value of 10 kHz within the range of 1–2 MHz.

The uniqueness of the outputs are analysed with three different parameters defined in [20] to determine the independence of CRPs, which is the most important quality factor for the proposed CRP enhancement methods. The first quality metric for uniqueness, U_QM1, is the Hamming distance (HD) of the outputs, which has an ideal value of 0.5. It can be defined as

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

where k is the total number of outputs, n is the output bit length and R_i is the ith output.

The second quality factor, U_QM2, checks how close the distribution of HDs is to a Gaussian distribution. U_QM2 has an ideal value of 1 and can be defined as

$$U\_\text{QM2} = \text{Corr}(\text{DIS\_HD},\ \text{Gaus}(Mn(\text{HD\_PUF}),\ \sigma)) \qquad (3)$$

where HD_PUF and σ are the mean and standard deviation of HDs of the collected data, respectively, DIS_HD is the distribution of HDs of the collected data and Corr is the correlation function. The closer the U_QM2 is to 1, the better distribution the outputs exhibit; hence, a better quality design is obtained.

U_QM3 is the quality metric that evaluates the uniqueness of the outputs according to the Gilbert–Varshamov bound. U_QM3 depends on the minimum HD of output pairs in a set of outputs. Bigger values for this metric indicate a higher-quality design.

Uniqueness analysis results of the f_{thp} selection method are shown in Fig. 5. As seen from this figure, U_QM1 is close to the ideal value of 0.5 for the three structures, for all f_{thpdif} values investigated. In spite of this, U_QM2 is slightly lower than the ideal value for the 5-stage and 11-stage RO structures and it is significantly lower than the ideal value for the 21-stage RO structure. U_QM3 is very low for all the structures when an f_{thpdif} value of 10 kHz is used. For f_{thpdif} values of 25, 50, 100 and 200 kHz, the results are

doi: 10.1049/iet-cds.2014.0089

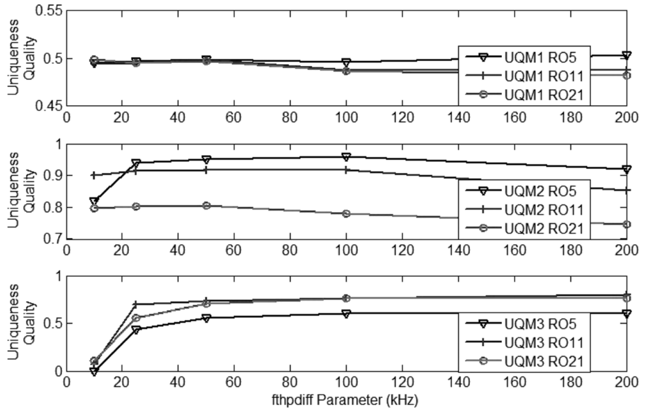


Fig. 5 *Uniqueness quality against f_{thpdif} parameter*

Table 1 f_{thp} selection method area consumption against CRP count

Largest f_{thp}	Required RO number	Area increase, %	CRP count
1	88	0	1
1.2	100	13	9
1.4	110	25	17
1.6	119	35	25
1.8	132	50	33
2	145	64	41

close to each other. Uniqueness results confirm the validity of the method. Since the results are similar for 25, 50, 100 and 200 kHz, using the smaller f_{thpdif} value is better for creating more CRPs with minimum area, time and power consumption. In addition to this, all analysed RO structures with different number of stages exhibit acceptable levels of uniqueness. Therefore using the one with five stages is the best choice for area, time and power efficiency of the system.

Next, the area efficiency of the method is analysed using the five-stage RO structure. For this purpose, area overhead against CRP count is evaluated using an f_{thpdif} value of 25 kHz and f_{thpmin} value of 1 MHz, which seem to be the optimum values according to the analysis described above for the specific PUF design, FPGA type and technology node. Area requirement of the system is measured for an output length of 128 bits using different f_{thpmax} values. As seen from Table 1, the area overhead is limited to 35 and 64% for supplying 25 and 41 CRPs, respectively.

5 Enhanced CRP set with RO selection method

Another possible approach to enhance the CRP set is to change the RO frequencies that are used by the DP to generate the PUF outputs. This can be done by implementing more ROs than the minimum required number and selecting a subset of these ROs according to the applied challenge to apply the DP-based grouping method. Let $\mathrm{RO}_{\mathrm{min}}$ be the minimum number of ROs to generate output with a certain bit length and f_{thp} value, and let $\mathrm{RO}_{\mathrm{imp}}$ be the number of implemented ROs in the system. In this case, the first part of the DP algorithm until the sorting step is updated as presented in (Algorithm 1). With this update, DP selects the $\mathrm{RO}_{\mathrm{min}}$ number of ROs out of $\mathrm{RO}_{\mathrm{imp}}$ number of ROs that are already implemented in the system depending on the applied challenge. When the selection is completed, the algorithm remains unchanged starting from the sorting step.

```
Algorithm 1: Revised part of the DP approach in pseudo code
Data:

1. $\mathrm{RO}_{\mathrm{min}}$ number of random RO selection information applied as challenge.
2. $f_{\mathrm{thp}}$ for robustness.

Choose $\mathrm{RO}_{\mathrm{min}}$ number of ROs with their frequencies measured under nominal operating conditions and form a linked list, FreqRO[$n$].
Result: Groups of ROs.
```

In this case, the number of different RO sets composed of $\mathrm{RO}_{\mathrm{min}}$ out of $\mathrm{RO}_{\mathrm{imp}}$ ROs can be calculated as

$$C(\mathrm{RO}_{\mathrm{imp}},\ \mathrm{RO}_{\mathrm{min}}) = \frac{\mathrm{RO}_{\mathrm{imp}}!}{\mathrm{RO}_{\mathrm{min}}!(\mathrm{RO}_{\mathrm{imp}} - \mathrm{RO}_{\mathrm{min}})!} \tag{4}$$

which increases factorially with $\mathrm{RO}_{\mathrm{imp}}$ when the $\mathrm{RO}_{\mathrm{min}}$ is constant. In this method, $\mathrm{RO}_{\mathrm{min}}$ number of selected RO identities acts as a challenge and the PUF output acts as the response. Since the possible number of RO subsets increases factorially, the number of possible CRPs increases similarly, which is a desired property that is not presented for RO-PUFs previously.

The drawback of this method is the possible similarity of the groups after the DP is applied. This may occur if most of the ROs within the two subsets are the same. The proposed solution for this problem is to generate more RO subsets than the system's CRP requirement and use the sets that are quite different from each other as challenges. In addition to this, if the number of possible sets is much

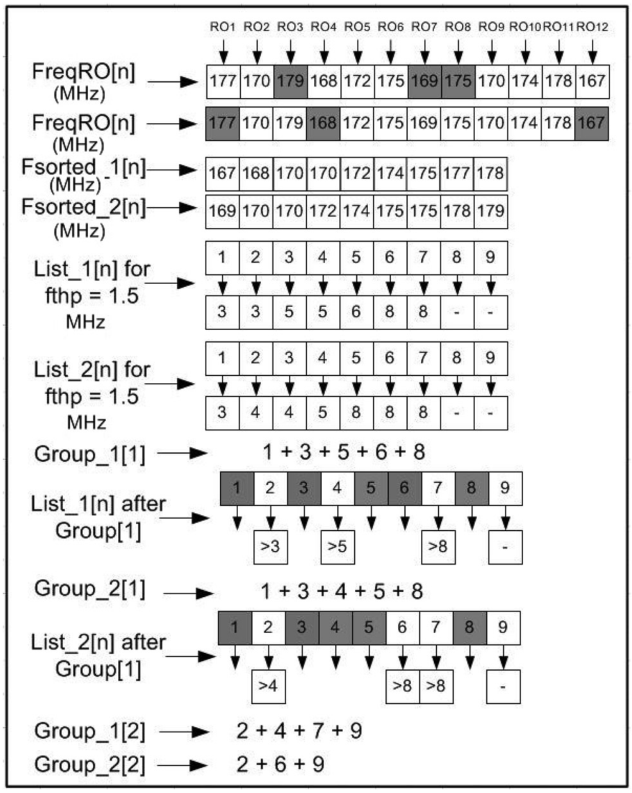


Fig. 6 *DP sample execution for RO selection method*

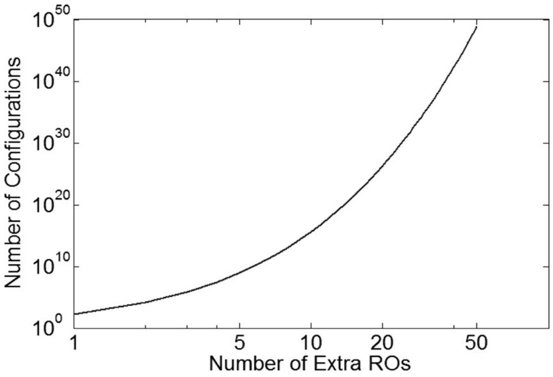


Fig. 7 *Number of CRPs against additional ROs*

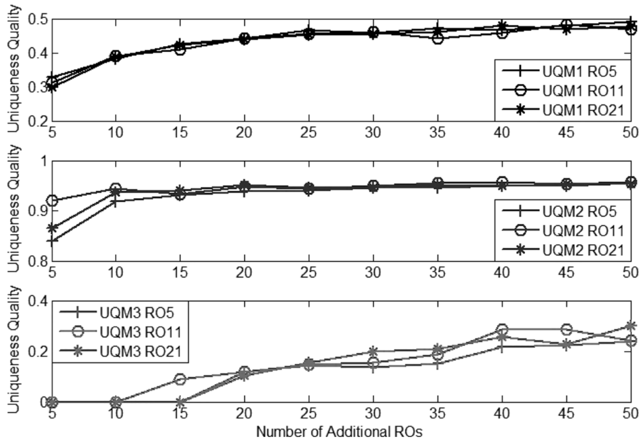


Fig. 8 *Uniqueness quality against additional ROs*

bigger than the CRP requirement, random selection of the challenges will have a small probability of creating similar outputs. This situation is analysed with real implementation results at the end of this section.

To verify the effectiveness of the RO selection method, Example 1 given in Section 3 is repeated for two RO subsets composed of nine ROs each that are selected from the whole RO set of 12 ROs. An f_{thp} value of 1.5 MHz is used for the analysis again. As seen in Fig. 6, two different RO selections resulted in different groupings when the DP is applied. This verifies the effectiveness of the RO selection method for enhancing the CRP set in ordering-based RO-PUFs.

CRP generation capability of the RO selection method is illustrated in Fig. 7 by calculating the number of possible configurations for each additional RO within an RO-PUF of 160 ROs. The number of possible CRPs increases factorially with the number of additional ROs. Even adding five ROs results in more than 10^{10} different combinations and this number exceeds 10^{50} when 50 ROs are added to the system.

Table 3 Minimum HD among 128 bit outputs within 10 000 CRPs based on the number of ROs

Number of ROs	Minimum HD among 128 bit output	Area overhead
165	0	0.031
170	0	0.063
175	0	0.094
180	2	0.125
185	6	0.156
190	10	0.188
195	11	0.219
200	15	0.25
205	18	0.281
210	22	0.313

Analysis of the RO selection method is performed by creating ten different RO sets composed of 165–210 ROs for three different RO structures composed of 5, 11 and 21 stages in MATLAB environment, similar to the manner described in the previous section. Then, 10 000 subsets from each of these sets are created by selecting 160 ROs randomly, and DP is applied to the subsets to generate 128 bit long outputs. As a result, 10 000 PUF outputs for each RO set is generated. The parameters defined in [20] and explained in the previous section, U_QM1, U_QM2 and U_QM3, are used to analyse the uniqueness of the outputs. As seen in Fig. 8, uniqueness of the outputs increases with increasing number of additional ROs for all three structures. U_QM1 reaches 0.95 and U_QM2 reaches 0.45 by adding only 20 ROs to the system, which are quite close to the targeted values of 1 and 0.5, respectively. U_QM3 shows that adding fewer than 20 ROs may result in generating identical responses to different challenges within a set of 10 000 CRPs.

When the results of the two proposed methods are compared, it is observed that U_QM3 is significantly lower in the RO selection method. This indicates that some output pairs generated with the RO selection method are closer to each other than the ones generated with the f_{thp} selection method. The probability of output pairs that have more than a certain level of HD may be beneficial from a system designer's perspective. For this purpose, the probability of output pairs with an HD of fewer than 10 to 50 bits is calculated for each RO set of the 5-stage structure and presented in Table 2. As the number of additional ROs increases, the probability of output pairs with low HD decreases as expected. For instance, when a total of 210

Table 2 Probability of output couples with HD less than the minimum HD defined

Number of ROs	Minimum HD ≤ 10	Minimum HD ≤ 20	Minimum HD ≤ 30	Minimum HD ≤ 40	Minimum HD ≤ 50
165	4×10^{-2}	1.4×10^{-1}	2.7×10^{-1}	4.11×10^{-1}	6.06×10^{-1}
170	3.8×10^{-3}	2.5×10^{-2}	8.4×10^{-2}	2.2×10^{-1}	4.8×10^{-1}
175	2.9×10^{-4}	3.7×10^{-3}	2.2×10^{-2}	9.8×10^{-2}	3.1×10^{-1}
180	8.3×10^{-6}	4.8×10^{-4}	6.8×10^{-3}	4.7×10^{-2}	2.1×10^{-1}
185	6.4×10^{-7}	4.7×10^{-5}	1×10^{-3}	1.2×10^{-2}	1×10^{-1}
190	8×10^{-8}	2.3×10^{-5}	8.1×10^{-4}	1.3×10^{-2}	1.27×10^{-1}
195	6×10^{-8}	6.6×10^{-6}	2.95×10^{-4}	6.6×10^{-3}	8×10^{-2}
200	0	5×10^{-7}	7.6×10^{-5}	4×10^{-3}	7.8×10^{-2}
205	0	4.4×10^{-7}	5.1×10^{-5}	2.3×10^{-3}	4.9×10^{-2}
210	0	0	7.44×10^{-6}	5.8×10^{-4}	2.3×10^{-2}

doi: 10.1049/iet-cds.2014.0089

ROs are implemented, none of the output pairs within the 10 000 outputs have an HD of ≤20 bits. Moreover, almost 98% of output pairs have an HD of more than 50 bits.

Another analysis performed on the proposed method is determining the minimum HD within the output pairs. This is meaningful if the target system has a minimum HD requirement within the responses. Hence, the system designer can choose the optimum number of ROs that should be implemented in order to simultaneously maintain the required quality of the outputs and the minimum area consumption. Results of the indicated analysis and the area overhead of the RO selection method are presented in Table 3.

6 Comparison of the f_{thp} selection and RO selection methods

Both the f_{thp} selection and RO selection methods provide CRP support to ordering-based RO-PUFs. However, they have different behaviours in terms of CRP count and quality, area, time and power efficiency. Therefore a comprehensive comparison of the proposed methods is presented in this section. For this purpose, an ordering-based RO-PUF without CRP support and two ordering-based RO-PUFs with CRP support that are based on f_{thp} selection and RO selection methods are compared and the results are presented in Table 4. In this comparison, f_{thp} selection method with 41 CRP generation capability and RO selection method with 10^{50} CRP generation capability are compared. One of the main performance parameters of PUF structures is area consumption. As can be seen from this table, ordering-based RO-PUF without CRP support requires 88 ROs, whereas CRP supporting structures with f_{thp} selection and RO selection require 145 and 210 ROs, respectively. Another important performance parameter is output generation time, which is directly proportional to the number of ROs to be measured during the output generation and measurement time for each RO. About 81 µs is used for the measurement time of each RO, since it is the optimum measurement time according to the analysis presented in [21]. As can be seen from this table, ordering-based RO-PUF without CRP support requires 7.2 ms to measure 88 ROs, whereas CRP supporting structures with f_{thp} selection and RO selection require 11.9 and 13.1 ms to measure 145 and 160 ROs, respectively. Even though the structure with RO selection method has 210 ROs implemented, only 160 of them will be measured, since the DP will only use the frequencies of the selected ROs. Power consumption of the RO structures is also directly proportional to the number of ROs to be measured; hence, output generation time. Uniqueness analysis of the CRPs is also presented for the proposed methods for the three metrics used in the literature.

Table 4 Comparison of ordering-based RO-PUFs in terms of response uniqueness

	Ordering-based RO-PUF CRP non-supported	Ordering-based RO-PUF f_{thp} selection	Ordering-based RO-PUF RO selection
CRP count	1	41	10^{50}
area (RO count)	88	145	210
output generation time, ms	7.2	11.9	13.1
U_QM1	N/A	0.4972	0.4925
U_QM2	N/A	0.953	0.954
U_QM3	N/A	0.46	0.2387

Even though the number of CRPs provided with the f_{thp} selection method is limited, uniqueness quality of the outputs is very good and the area overhead of the system is reasonable. This method is very convenient especially for applications that use PUF for secret key generation, that require highly unique outputs and reconfiguration of the keys for a limited number of times within the lifetime of the IC.

The main advantage of the RO selection method is its capability of generating highly unique and very large number of CRPs with an acceptable area overhead. The method is also very flexible and can be customised for the desired number of CRPs and uniqueness of the outputs, using the analysis presented above. RO selection method is very convenient especially for applications that use PUF for authentication purposes.

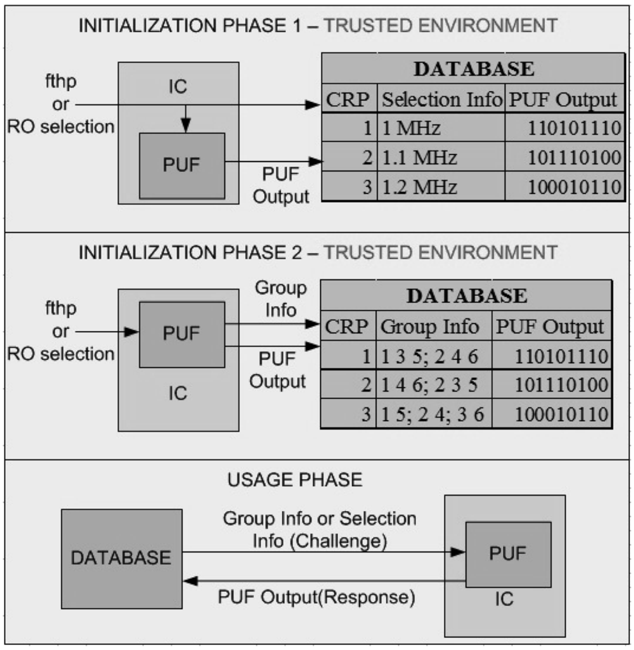
As discussed in this section, f_{thp} selection and RO selection methods have their own advantages and disadvantages. To achieve a better PUF design that is suitable for a bigger variety of applications, it is possible to combine both of these methods. In this case, both f_{thp} selection and RO selection information will be applied as challenges to the DP algorithm. With this approach, higher uniqueness levels and CRP count can be achieved by utilising the features of the f_{thp} selection and RO selection methods. However, using both of the methods at the same structure does not increase the total number of CRPs available, since the CRP set of the RO selection method is a superset of the CRP set of the f_{thp} selection method. This means that the groups formed using different f_{thp} values can also be formed via RO selection method as well. Therefore the advantage of combining the methods will be the ability of achieving higher uniqueness levels by applying different f_{thp} values when required.

7 Secure usage scenarios for ordering-based RO-PUFs

The main usage area of PUF circuits is security applications, which require end-to-end safety of the protected assets. This makes a vulnerability analysis of the system to possible threats inevitable. In this sense, the PUF circuit utilised by the application should maintain the CRP properties defined in Section 2 in order to ensure security. Before examining the proposed methods in terms of required CRP properties, general working principles of PUF circuits with CRP behaviour should be studied.

Ordering-based RO-PUF circuits that support CRPs have two main phases in their lifetime. First is the initialisation phase, where the required number of challenges is sent to the circuit and the generated responses are collected and saved by the authority. It is assumed that this phase takes place in a trusted environment; hence no security threats are possible, since the circuit is not publicly available and the CRP collection process is done either in the manufacturing facility or by the authority itself. Here, the authority can be defined as the security enforcer of the application, such as the credit card centre of a bank.

For the proposed methods used in ordering-based RO-PUFs, two different schematics can be used for the initialisation phase. In the first schematic, f_{thp} values or RO selection information depending on the CRP method preferred is used as the challenge and sent to the PUF circuit and the outputs are collected and recorded as the



DATABASE

CRP	Selection Info	PUF Output
1	1 MHz	110101110
2	1.1 MHz	101110100
3	1.2 MHz	100010110

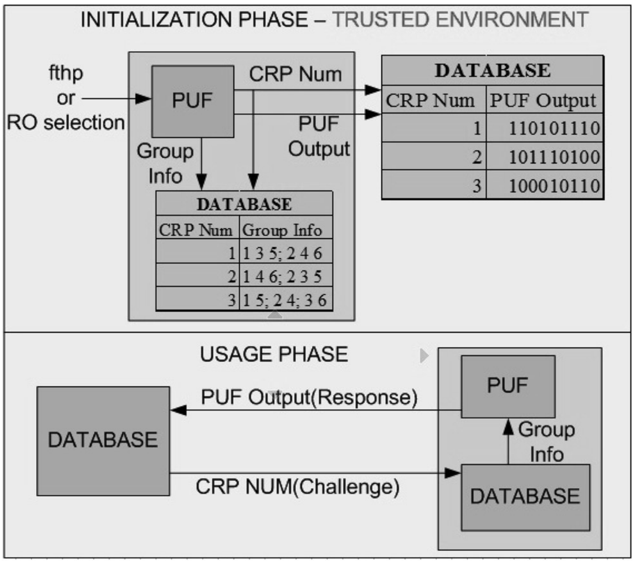
DATABASE

CRP	Group Info	PUF Output
1	1 3 5; 2 4 6	110101110
2	1 4 6; 2 3 5	101110100
3	1 5; 2 4; 3 6	100010110

Fig. 9 *Secure usage Scenario 1*

responses. In the second schematic, again f_{thp} values or the RO selection information are sent to the PUF circuit, but both the information on the formed groups and the output is sent to the authority. In this case, the grouping information is recorded as challenges and the outputs are recorded as the responses.

The second phase in the lifetime of PUF circuits is the usage phase. In this phase, one of the previously recorded challenges is sent to the circuit and the response is compared with the one in the database by the authority. One main difference arises because of the schematic selected in the initialisation phase. If the first schematic is used, f_{thp} values or the RO selection information are sent as the challenge to the device. Using the information received, DP is applied to the RO frequencies collected on the fly and output is generated according to the grouping information formed by the DP. If the second schematic is utilised and grouping information is sent to the device as the challenge, the need for running DP by the PUF circuit is avoided, minimising the time and power consumption in this phase. Another advantage of the second schematic is eliminating the need for implementing DP on IC. Since the DP is used only in the initialisation phase, it can be applied by the authority after collecting the RO frequencies from the IC. The critical point in this scheme is accessing to the RO frequencies should be limited to the initialisation phase. Otherwise, an attacker can record the RO frequencies and calculate all responses to challenges that the authority sent. Both initialisation phases and usage phase are illustrated in Figs. 9–11. Since two methods have two possible usage schematics, a total number of four combinations are present for the CRP enhanced ordering-based RO-PUFs.



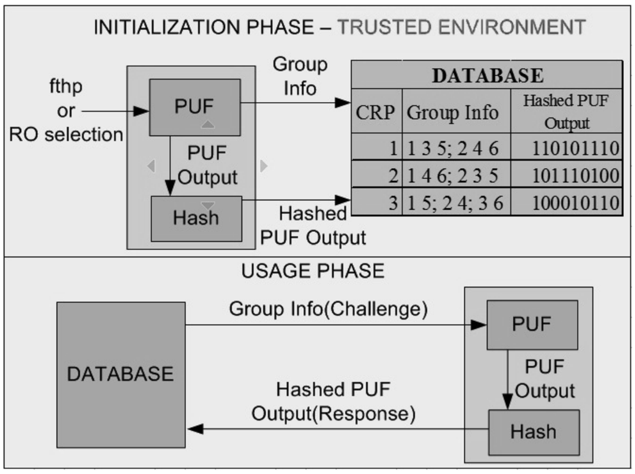
DATABASE

CRP Num	Group Info
1	1 3 5; 2 4 6
2	1 4 6; 2 3 5
3	1 5; 2 4; 3 6

DATABASE

CRP Num	PUF Output
1	110101110
2	101110100
3	100010110

Fig. 10 *Secure usage Scenario 2*



DATABASE

CRP	Group Info	Hashed PUF Output
1	1 3 5; 2 4 6	110101110
2	1 4 6; 2 3 5	101110100
3	1 5; 2 4; 3 6	100010110

Fig. 11 *Secure usage Scenario 3*

For a secure system that utilises the proposed methods, CRP properties stated in Section 2 should be maintained. When the ordering-based RO-PUF circuits are considered, CRP property numbers 2, 3 and 4 are satisfied inherently. However, the first CRP property is not satisfied for 3 out of 4 schematics and hence the security of the system is threatened. For the schematics that use grouping information in both proposed methods, the PUF circuit will have similar responses to challenges that have similar RO groups, violating the indicated CRP property stated above. Similarly, if the RO selection information is used as the challenge, similar RO sets may generate closely related outputs. The only exception for the violation of the first CRP property is using the f_{thp} values as challenges. Since it is assured that every f_{thp} value will generate distinct outputs, information leakage will not occur within different CRPs in this particular case.

To solve the information leakage problem that violates the required CRP properties, three different solutions are proposed. The first solution is to use a secure channel for sending the challenges and receiving the responses during the usage phase. Since an attacker will not be able to access the CRPs, the system will be secure with this method. An example of a secure channel is the secure layer formed between PCs and bank servers, where all the information exchanged is encrypted. The only disadvantage of this method is the cost of forming the secure channel.

In the second solution proposed, CRP ID and the grouping or selection information are stored on a NVM on IC and CRP ID and the PUF output are stored in the database of the authority, as illustrated in Fig. 10. In this scheme, only the

doi: 10.1049/iet-cds.2014.0089

Table 5 Comparison of secure usage scenarios

Scenario number	Advantages	Disadvantages
1	no NVM requirement no hash requirement	secure channel requirement
2	no secure channel requirement no hash requirement	NVM requirement
3	no secure channel requirement no NVM requirement	hash requirement

CRP ID is sent to device as the challenge and the PUF output is received as the response in the usage phase. The required information for output generation is picked up from the NVM depending on the CRP ID. Since the critical information, such as grouping data, will not leave the IC, CRPs will not leak information about each other and the system will be fully secure. The disadvantage of this method is the requirement for an NVM, which increases the cost. This solution may be very convenient for systems that already include NVMs, such as smart cards.

The third solution proposed excludes the need for a secure channel and NVMs by adding a hash function to the system that is utilised in the initialisation and usage phases, as shown in Fig. 11. In this method, grouping or selection information of ROs is used as the challenge and the hashed PUF output is used as response. CRPs are recorded to the database of the authority and PUF outputs are hashed each time the circuit is used. Since the hash function removes the direct relation between the challenges and responses, none of the CRP pairs give information about other pairs. Even though a hash function may be seen as an important overhead in the system, it can be implemented in software as well. In addition to this, since hash functions have a wide range of application areas, many systems that utilise PUF circuits may already contain them.

Advantages and disadvantages of the secure usage scenarios proposed for the CRP enhanced ordering-based RO-PUFs are summarised in Table 5. Depending on the area and timing requirements, and the available resources of the target system, the most convenient structure can be utilised without endangering the system security.

8 Conclusion

The number of CRPs a PUF circuit support is critical for security applications such as authentication. Ordering-based RO-PUFs are very efficient PUF structures with 100% robustness. However, CRP concept was not defined for them prior to this paper. We have developed two CRP enhancement methods for ordering-based RO-PUFs based on f_{thp} selection and RO selection. According to the analysis applied, uniqueness results of the f_{thp} selection method are better than the results of the RO selection method. However, RO selection method supplies a large number of CRPs with higher area, power and time efficiency. In addition to these, three secure usage scenarios, which prevent the CRPs leak information about each other are presented. With the proposed methods, secure, highly efficient and robust PUF circuits with a large number of CRP support become available.

References

1 Pappu, R.S.: 'Physical one-way functions'. PhD dissertation, Massachusetts Institute of Technology, Massachusetts, 2001

2 Suh, G.E., Devadas, S.: 'Physical unclonable functions for device authentication and secret key generation'. Design Automation Conf. (DAC), 2007, pp. 9–14

3 Maiti, A., Schaumont, P.: 'Improving the quality of a physical unclonable function using configurable ring oscillators'. Int. Conf. on Field Programmable Logic and Applications (FPL), 2009, pp. 703–707

4 Lim, D., Lee, J., Gasend, B., Suh, G.E., Dijk, M.V., Devadas, S.: 'Extracting secret keys from integrated circuits', *IEEE Trans. VLSI Syst.*, 2005, **13**, (10), pp. 1200–1205

5 Gassend, B., Clarke, D., Dijk, M.V., Devadas, S.: 'Delay-based circuit authentication and applications'. ACM Symp. on Applied Computing, 2003, pp. 294–301

6 Gassend, B.: 'Physical random functions'. MS thesis, Massachusetts Institute of Technology, Massachusetts, 2003

7 Guajardo, J., Kumar, S., Schrijen, G., Tuyls, P.: 'FPGA intrinsic PUFs and their use for IP protection'. 18th Annual Computer Security Applications Conf. (CHES), 2007, vol. 4727, pp. 63–80

8 Guajardo, J., Kumar, S., Maes, R., Schrijen, G., Tuyls, P.: 'Extended abstract: the butterfly PUF protecting IP on every FPGA'. Hardware-Oriented Security and Trust (HOST), 2008, pp. 67–70

9 Suzuki, D., Shimizu, K.: 'The glitch PUF: a new delay-PUF architecture exploiting glitch shapes'. Cryptographic Hardware and Embedded Systems (CHES), 2010, pp. 366–382

10 Maes, R., Rozic, V., Verbauwhede, I., Koeberl, P., van der Sluis, E., van der Leest, V.: 'Experimental evaluation of physically unclonable functions in 65 nm CMOS'. Proc. of the ESSCIRC, 2012, pp. 486–489

11 Lee, J.W., Lim, D., Gassend, B., Suh, G.E., Dijk, M., Devadas, S.: 'A technique to build a secret key in integrated circuits for identification and authentication applications'. Symp. on VLSl Circuits Digest of Technical Papers, 2004

12 Wang, X., Tehranipoor, M.: 'Novel physical unclonable function with process and environmental variations'. Design, Automation Test in Europe Conf. Exhibition (DATE), 2010, 2010, pp. 1065–1070

13 Maiti, A., Schaumont, P.: 'Improved ring oscillator PUF: an FPGA-friendly secure primitive', *J. Cryptol.*, 2011, **24**, (2), pp. 375–397

14 Yin, C., Qu, G.: 'Temperature aware cooperative ring oscillator PUF'. IEEE Int. Workshop on Hardware Oriented Security and Trust (HOST), 2009, pp. 36–42

15 Ruhrmair, U., Solter, J., Sehnke, F.: 'On the foundations of physical unclonable functions'. Cryptology ePrint Archive, 2009, vol. 277

16 Yin, C., Qu, G.: 'LISA: maximizing RO-PUF's secret extraction'. IEEE Int. Symp. on Hardware Oriented Security and Trust (HOST), 2010, pp. 100–105

17 Komurcu, G., Pusane, A.E., Dundar, G.: 'Dynamic programming based grouping method for RO-PUFs'. Ninth Conf. on Ph. D. Research in Microelectronics and Electronics (PRIME), 2013, pp. 329–332

18 Gassend, B., Clarke, D., Dijk, M.V., Devadas, S., Lim, D.: 'Identification and authentication of integrated circuits', *Concurrency Comput. Pract. Exp.*, 2004, **16**, (11), pp. 1077–1098

19 Majzoobi, M., Koushanfar, F.: 'Techniques for design and implementation of secure reconfigurable PUFs', *ACM Trans. Reconfigurable Technol. Syst.*, 2009, **2**, (1), pp. 1–33

20 Komurcu, G., Dundar, G.: 'Determining the quality metrics for PUFs and performance evaluation of two RO-PUFs'. IEEE Tenth Int. New Circuits and Systems Conf., (NEWCAS), 2012, pp. 73–76

21 Komurcu, G., Pusane, A., Dundar, G.: 'Analysis of ring oscillator structures to develop a design methodology for RO-PUF circuits'. IFIP/IEEE 21st Int. Conf. on Very Large Scale Integration (VLSI-SoC), 2013, pp. 332–335

doi: 10.1049/iet-cds.2014.0089