Physical Unclonable Function-based Key Sharing for IoT Security

Jiliang Zhang, Member, IEEE

Abstract—In many Internet of Things (IoT) applications, resources like CPU, memory, and battery power are limited and cannot afford the classic cryptographic security solutions. Silicon Physical Unclonable Function (PUF) is a lightweight security primitive that exploits manufacturing variations during the chip fabrication process for key generation and/or device authentication. Ring Oscillator (RO) PUF as one of the most popular silicon weak PUFs can generate secret bits by comparing the frequency difference between any two ROs. Previous RO PUFs improve flexibility and reliability through adding redundant ROs, which incurs unacceptable hardware overheads. In addition, traditional weak PUFs such as RO PUF generate chip-unique key for each device, which restricts their application in security protocols where the same key is required to be shared in resource-constrained devices. In order to address these shortcomings, we propose a crossover RO PUF (CRO PUF) that improves flexibility, reliability and reduces hardware overheads. It is the first PUF that can generate the shared key in physically. The basic idea is to implement one-to-one input-output mapping with Lookup Table (LUT)-based interstage crossing structures in each level of inverters. Individual customization on configuration bits of interstage crossing structure and different RO selections with challenges bring high flexibility. Therefore, with the flexible configuration of interstage crossing structures and challenges, CRO PUF can generate the same shared key for resource-constrained devices, which enables a new application for lightweight key sharing protocols. Experimental results show that our proposed PUF structure has much lower hardware overheads, better uniqueness and reliability than the previous configurable RO PUFs.

Index Terms—Physical unclonable function (PUF), ring oscillator, flexibility.

I. INTRODUCTION

A. Motivation

With the increasing demands of security, privacy protection, and trustworthy computing, key generation and device authentication become two of the most challenging design concerns, particularly for systems such as smart cards, sensors, and smart phones where the lack of persistent power limits the duration of countermeasure enforcement [1]. Traditional security mechanisms store secret keys in electrically erasable programmable read-only memory (EEPROM) or battery-backed non-volatile static random access memory (SRAM), and combine cryptographic algorithms to implement information encryption and authentication. In order to secure cryptographic key storage, tamper-resistant devices with a number of countermeasures to defeat various kinds of physical attacks are developed. However, in many IoT applications, resources like CPU, memory, and battery power are limited so that they cannot afford the classic cryptographic security solutions. Silicon physical unclonable function (PUF) emerged as a new hardware primitive provides a unique device-dependent mapping from challenges to responses based on the unclonable properties of the underlying physical device for device authentication and key generation. The key generated by PUF can resist tampering attacks because the underlying nano-scale structural disorder will most likely be damaged during physical tampering. Therefore, PUF is a promising security primitive for Internet of Things.

There has been more than a decade of intensive study on PUFs since it was introduced in the research community [2]. Among PUFs of different forms, silicon PUFs [3] [4] are of the most interest in terms of fabrication cost and readiness to be integrated to computing and communication devices. Current silicon PUFs can be classed into strong PUFs and weak PUFs [1]. The security of strong PUFs is based on their high entropy content providing a huge number of unique challenge-response pairs (CRPs), which can be used in authentication protocols. On the other hand, weak PUFs exhibit only a small number of CRPs to be applied. Although they are not applicable to authentication protocols, the corresponding responses of weak PUFs can be used as a device-unique key or seed for conventional encryption systems, while maintaining the advantages of physical unclonability [1]. Arbiter PUF [7] is a typical strong PUF. SRAM PUF [9] and Glitch PUF [4]–[6] are typical weak PUFs. Ring oscillator (RO) PUF [8] can be used as both strong and weak PUF, but it only produces a limited number of CRPs which are not large enough for authentication. Therefore, RO PUF is more suitable for key generation. Besides, a RO PUF does not require high symmetry and thereby is more easily to be implemented on FPGAs than other PUFs such as Arbiter PUF. In past decades, PUFs have attracted much attention in academia and industry for various security related applications such as hardware IP protection [3] [25], device authentication [8] [30] [34] and software security [31].

B. Limitations of Prior Art

It is well-known that strong and weak PUFs enable a variety of security protocols such as authentication [21] and encryption/decryption [8]. However, current weak PUFs exhibit a
shortcoming when they are used in some security protocols. They generate the chip-unique key for each device and cannot be cloned in another device due to process variation, while some security protocols such as multi-party communication require many parties to share the same key. Therefore, current weak PUFs are inapplicable to such application scenarios.

In addition, as a typical weak PUF, RO PUF is based on the frequency difference among ROs to generate random bits. An RO is a simple circuit of a set of inverters connected in a loop with a particular frequency. The PUF generates logic-0 or logic-1 by comparing the frequencies of any two ROs. However, the delay difference caused by manufacturing process variation is sensitive to environment, which makes the PUF responses unreliable. The error correcting is a general technique for correcting flips in PUF responses for many PUF-related applications such as cryptographic key generator [22], IC metering [23] and FPGA IP protection [25]. For example, if the BCH (127, 64, 21) code is used, 10-bit errors in a 127-bit PUF output can be corrected and the probability of failing to re-generate a consistent output (false negative rates) is less than $5 \times 10^{-11}$ [8]. However, the overhead incurred by the ECC increases quadratically with the number of errors. Therefore, it is recommended to first use error reducing techniques to reduce the bit flips and then use error correcting techniques to correct any possible errors. Currently, many error reducing techniques have been proposed for RO PUF, but high hardware overhead is incurred. Therefore, effective low overhead error reducing techniques are in urgent need.

C. Our Contributions

In order to address above two issues, this work proposes a highly flexible configurable RO PUF, named Crossover RO PUF (CRO PUF). We first report the concept of CRO PUF in [24]. In this article, 1) CRO PUF-based key-sharing method is new proposed; 2) CRO PUF-based secure information transmission protocol is new proposed; 3) we elaborate the details of the proposed CRO PUF with illustrative example and in-depth discussion on shared-key generation, key-sharing protocol, and security vulnerabilities. The main contributions are as follows.

1) The flexible crossover RO PUF structure is proposed. The interstage crossing structure can choose different inverters in each level with input challenges and hence can drastically mitigate the effect of environment on PUF responses and generate more reliable responses.

2) CRO PUF-based key-sharing method and secure information transmission protocol are proposed. It is the first PUF that is able to generate the shared key in physically with the flexible configuration of challenges and inter-stage crossover structures, which enables the multi-party communication for adjacent resource-constrained nodes.

3) Experimental results based on the public PUF dataset [18] demonstrate that the CRO PUF has low hardware overhead, good uniqueness and high reliability.

The rest of this paper is organized as follows. Related work is elaborated in Section II. Section III gives a detailed introduction about our proposed crossover RO PUFs. The proposed CRO-based key-sharing is elaborated in Section IV. Potential security threats and countermeasures are analyzed in Section V. The detailed experimental results and analysis are reported in Section VI. Finally, we conclude in Section VII.

II. RELATED WORK

To improve reliability, the existing error reducing techniques incur high hardware overheads and hence make them difficult to be deployed in practice. In addition, traditional PUFs cannot generate the shared-key in physically for some security protocols. We will discuss in detail below.

A. Error Reducing Techniques

In order to improve reliability, 1-out-of-$n$ RO PUF was proposed [8]. The basic idea is to select two ROs with maximal frequency difference among $n$ ROs. However, 1-bit response will waste $(n - 2)$ ROs, which incurs unacceptable hardware overheads. Tang, Lin and Zhang [15] proposed a frequency offset-based reliability-enhancing technique for RO PUF. The key idea is to make the frequency difference larger than a given threshold by offsetting the frequencies of RO pairs to improve reliability. In [19], Paral and Devadas proposed to use string pattern matching to generate the PUF-based key without error correction to reduce hardware overhead. Yin and Qu [20] proposed a temperature aware collaboration (TAC) method for RO PUF to invert the unreliable bits into reliable ones by the cooperation between contributing RO pairs which may generate unreliable bits. Recently, majority voting methods [27] [28] that the minority is subject to the majority were proposed to improve PUF reliability effectively. For example, in [28], $n$ basic PUF units vote to generate 1-bit reliable response. Hence, 1-bit reliable response will waste $(n - 1)$ PUF units, which incurs high overhead for most of PUFs such as Arbiter PUF and RO PUF.

In addition to above methods, reconfigurable/configurable methods are most related to our work. Unlike traditional PUFs exhibiting a static challenge/response behavior, reconfigurable PUF exhibits dynamic unpredictable challenge/response behavior. In many practical applications such as resisting FPGA replay attacks [11], side-channel attacks [11], modeling attacks and man-in-the-middle attacks [12], we expect PUFs can exhibit the reconfigurable challenge/response behavior. The concept of reconfigurable arbiter PUF was first proposed by Lee et al [7]. They proposed to integrate a floating gate transistor into the delay lines of an arbiter PUF to physically change
the challenge/response behavior of the PUF based on a logical state maintained in non-volatile memory [11]. Lao and Parhi [13] proposed several reconfigurable silicon PUF structures to change the behavior of silicon PUF after deployment and also evaluated their reconfigurability by simulation. Recently, Zhang et al. [11] proposed to use reconfigurable PUFs to defeat the replay attack and tested two reconfigurable PUFs that exhibit high reconfigurability.

Similar to reconfigurable PUFs, configurable RO PUF is introduced by Maiti and Schaumont [10] to improve RO PUF reliability. As shown in Fig. 1 the key idea is that a $2 \times 1$ multiplexer is used to select one out of two inverters at each stage of the RO. This technique uses the configurations with the largest delay difference to improve the PUF reliability. Another highly flexible configurable RO PUF was proposed in [14]. The key idea is that a $2 \times 1$ multiplexer is used to select or bypass the inverter to improve the reliability of RO PUFs, as shown in Fig. 2. The configurations for RO pairs are to choose the largest delay difference to generate reliable PUF output. For these reconfigurable/configurable PUFs, the utilization ratio of multiplexers added in ROs is low, and the inverters are not fully used in some configurations.

B. PUFs for Shared-key Generation

In IoT, sensitive information needs to be transmitted to participants over a potentially insecure communication, so security features such as authentication and encrypted data transfer are required. However, it is difficult to secure IoT with security features used in traditional Internet [26]. In order to fit such application scenario, the deployed security features must be extremely lightweight. Instead of relying on heavyweight public-key primitives or secure storage for secret symmetric keys, PUF is a lightweight hardware primitive that can be directly integrated in cryptographic protocols. So far, all existing PUF-enable encryption/decryption protocols follow the same paradigm: PUFs generate the chip-unique key for each resource-constrained device and cannot be shared securely in another resource-constrained device. In this paper we consider application scenarios where PUF-enable encryption/decryption schemes fail to work: multi-party communication needs to share the same key. To our knowledge, PUFs for shared-key generation have not been reported in current references. We construct the first and efficient PUF-based security protocol for this setting. Therefore, this is the first work that PUFs can generate the same lightweight shared-key in physically for resource-constrained devices.

III. CROSSOVER RO PUF

In order to improve reliability, generate shared-key and resist potential attacks such as FPGA replay attacks, modeling attacks and man-in-the-middle attacks, we proposed a crossover RO PUF that has advantages over the previous configurable RO PUFs in terms of flexibility and reliability. Considering 1-out-of-N coding, an RO PUF is comprised of many ROs and the multiplexers select two of them to be compared with the comparator [1]. Previous configurable RO PUFs only use the single RO pair to implement configurability. Our proposed crossover RO PUF structure is much more flexible because we select every inverter from multiple RO pairs with Lookup Tables (LUTs).

A. The Architecture of Crossover RO PUF

Crossover RO PUF consists of ROs and crossover structure. An RO is composed of an odd number of inverters in a ring, whose output oscillates between two voltage levels, representing true and false. The inverters are attached in a chain and the output of the last inverter is fed back into the first one. Since a single inverter computes the logical NOT of its input, the output of the last inverter in a chain with an odd number of inverters is the logical NOT of the input of the first inverter. The output of the last inverter is asserted a finite amount of time after the input of the first inverter is asserted and the feedback of the last inverter to the first inverter causes oscillation. A circular chain composed of an even number of inverters cannot be used as a ring oscillator, because the output of the last inverter is the same as the input of the first inverter [29].

Fig. 3 depicts the crossover RO PUF architecture that shows the flexibility of selecting inverters in ROs. The crossover RO PUF has $n$ ROs and $m$ levels of inverters. Each RO consists of $m$ inverters with a particular frequency. The $m$ should be larger than 2, otherwise, the RO would oscillate too fast to be precisely counted by the counter. For $m$ levels of inverters, the outputs of previous inverter level are fed as the inputs to the next inverter level after interstage crossing. The interstage crossing cell determines the routing path of step signals input without any additional logical operation. There are $m-1$ interstage crossing cells to change the configuration of the delay loop with selection inputs.

As shown in Fig. 3 configuration selection $S = (S_1, S_2, ..., S_i, ..., S_{m-1})$, where $S_i$ has $[\log_2 n]$ bits and determines the connection order of inverter to the next inverter.
level in \(i\)-th stage; The configuration selection \(S\) and challenge are combined together as the whole challenge to be input into the CRO PUF for generating the response. \(S_{m-1}\) is dedicated to ensure closed loops. The number of possible different configurations of the delay loops is \((A^n_m)^{m-2}\). The level \(m\) must be an odd number and \(m > 2\) in order to make the delay loop form the oscillation, and it can determine the frequency level of the RO. The \(m\) is not directly related to \(n\). The \(n\) determines the number of possible challenges, while the \(m\) determines the frequency level of the ROs. The larger \(m\) which means more inverters in RO exhibits slower frequencies. In practical applications, the frequencies of ROs should not be too high and too low. If the frequency is too high, high-precision counter is required; if the frequency is too low, the time to generate response would be long, and hardware and power overhead would be increased. Usually, we can set \(m\) to 5 or 7 which is the empirical value that meets above requirements.

Under the precondition of ensuring a one-to-one mapping, the connection of inverters can be customized by the designers and users. After selecting inverters in each level, we can get a group of fixed sequence of RO pairs. Any two of ROs chosen by the challenge through multiplexers are connected to the clock input ports of the two counters to generate 1-bit PUF response by comparing the values read from the two counters within a period of time. The arbiter generates a logical 0 or 1 for this chosen RO pair depending on which RO has the higher frequency. By choosing different inverters to build ROs with input challenges, the delay difference for each pair of RO will generate more bits.

B. Interstage Crossing

In this section, we introduce a high flexibility interstage crossing with LUTs. Fig. 4(a) shows the internal structure of a 3-input LUT. An \(n\)-input LUT can be configured to implement any \(n\)-input logic function. For example, SRAM can be set with ‘00011011’ in initialization phase to implement the function \(A_0 \cdot A_2 + A_1 \cdot A_2\), and set with ‘00100111’ to implement \(A_0 \cdot A_2 + A_1 \cdot A_2\). By configuring SRAM, we can easily get the logic function required in interstage crossing. Fig. 4(b) gives an example of a 4-bit crossing network with 6-input LUTs. Each LUT takes \(A, B, C, D\) as 4-bit inputs and the rest two inputs as the selection imports. If the selection bits are configured as 00,01,10,11, the output of the LUTs will be \(A, B, C, D\). In the same way, the output of the LUTs will be shuffled as \(B, C, D, A\) when selection bits are 01,10,11,00.

Since the data inputs and outputs of all the interstage crossing must form a one-to-one mapping, no duplicated outputs are allowed in the network. In addition, even though adversaries can get all configuration bits from the SRAM of LUTs in interstage crossing, they cannot get any delay information of inverters and hence cannot derive the responses.

Considering the influence of delay added in interstage crossing, the existing FPGA design tools can minimize the delay-skew between a pair of routes, but they do not guarantee the structural symmetry \[16\]. For example, the multiplexers and inverters in a configurable RO PUF will be connected to the switch matrix which uses routes with different lengths depending on the individual placements. So if the manufacturing process variation is insufficient to offset it, the interstage crossing structure could make entire PUF circuit be highly biased. Our method can set all connections of inverters by configuring SRAM without impacting the routing in switch matrixes. It means LUT-based interstage crossing has high flexibility to improve PUF reliability.

C. Flexibility and Reliability

Our proposed crossover RO PUF can get larger frequency differences between ROs than previous reconfigurable PUFs and hence generate more reliable PUF responses. In what follows, we give an example to explain the advantage.

As shown in Fig. 5, consider \(4 \times 5\) ROs have 4 rows inverters, \(RO_1\) to \(RO_4\), and each consists of 5 inverters. Assuming the delays of these inverters are: \{\(a_1 = 3, a_2 = 6, a_3 = 8, a_4 = 7, a_5 = 5\)\}, \{\(b_1 = 9, b_2 = 7, b_3 = 4, b_4 = 5, b_5 = 5\)\}, \{\(c_1 = 5, c_2 = 4, c_3 = 6, c_4 = 6, c_5 = 5\)\}, \{\(d_1 = 2, d_2 = 5, d_3 = 6, d_4 = 4, d_5 = 3\)\}. Where \(a_i\) to \(d_i\) denote the delay of the \(i\)-th inverter from \(RO_1\) to \(RO_4\), respectively. The total delays of four ROs are:

\[
D_{RO1} = 3 + 6 + 8 + 7 + 5 = 29 \\
D_{RO2} = 9 + 7 + 4 + 5 + 5 = 30 \\
D_{RO3} = 5 + 4 + 6 + 6 + 5 = 26 \\
D_{RO4} = 2 + 5 + 6 + 4 + 3 = 20
\]
When using decoupled neighbor coding, RO is 1 unit of time slower than RO₂, and RO₃ is 6 units of time faster than RO₄. The delay difference can be up to 10 units of time with 1-out-of-n coding method [8]. Generally, a large delay difference can generate a reliable bit. With the ingenious selection in crossover structure, \( \{b_1, b_2, a_3, a_4, a_5\}, \{a_1, d_2, c_3, b_4, b_5\}, \{c_1, a_2, d_3, c_4, c_5\} \) and \( \{d_1, c_2, b_3, d_4, d_5\} \) are used to build RO₁ to RO₄. The delay difference becomes 12 (RO₁ and RO₂) and 11 (RO₃ and RO₄) units of time. The largest delay difference is 19 units of time, which is about twice as large as the delay difference when there is no interstage crossing in the ROs. The delay of each inverter is unpredictable due to fabrication variation. Any inverter in an RO is faster or slower than the inverter at the same position in another RO with equal probability.

In the above example, although \( \{a_1, a_2\} \) in RO₁ is slower than \( \{b_1, b_2\} \) in RO₂, the total delay difference will be reduced when including the rest inverters. When reconfiguring RO with the interstage crossing, we can choose inverters ingeniously to increase the gap of total delay between two ROs, which makes the outputs more reliable.

IV. CRO PUF-based Key-sharing

A. Principle of Shared-key Generation

The shared key is required in multi-party communication between different devices. Traditional PUFs generate chip-unique key for every device, while CRO PUF is able to generate the same shared key for all devices. Therefore, CRO PUF is suitable for one-to-many authentication. CRO PUF is based on the inter-stage crossover structure which can be configured with the SRAM value. Different devices can produce the same response as the shared key with the appropriate configurations and challenges. For a CRO PUF with \( n \) rows and \( m \) columns, there are \((m-1)\cdot[\log_2 n]\)-bit selection signals which have \((A_n^m)^{m-2}\) combinations. The challenge \( C \) can have up to \( A_n^m \) different selections with the multiplexers to select any two ROs for frequency comparison. With the increasing of \( n \) and \( m \), the number of the selection signals and the challenges increases exponentially. In addition, the number of configurations of inter-stage crossover structures provides high flexibility for one-to-many authentication. The delay model of a CRO PUF with \( n \) rows with \( k \) inverters is shown as follows.

\[
\text{Delay}_{RO} = \begin{bmatrix}
d_{11} & d_{12} & \ldots & d_{1j} & \ldots & d_{1k} \\
d_{21} & d_{22} & \ldots & d_{2j} & \ldots & d_{2k} \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
d_{11} & d_{12} & \ldots & d_{ij} & \ldots & d_{ik} \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
d_{n1} & d_{n2} & \ldots & d_{nj} & \ldots & d_{nk}
\end{bmatrix}
\]

The delay vector of each line \( D_{RO} = \{D_1, D_2, \ldots, D_i, \ldots, D_n\} \), where \( D_i = \sum_{j=1}^{k} d_{ij} \). The selection signal \( S = (S_1, S_2, \ldots, S_j, \ldots, S_{k-1}) \), where \( S_j \) controls the connection path between the \( j \)-th and \( (j+1) \)-th column inverters, i.e.,

\[
\{d_{1j}', d_{2j}', \ldots, d_{nj}'\} = f(d_{1j}, d_{2j}, \ldots, d_{nj})
\]

The challenge \( C_{RO} \) is used to choose different rows of ROs for the frequency comparison, i.e,

\[
\{D_1', D_2'\} = g(D_1, D_2, \ldots, D_n)
\]

The selection signal \( S \) adjusts the delay of each column with the function \( f \). Challenge uses the function \( g \) to select different rows of ROs for comparison to generate the response. The delay is different between any two CRO PUFs, but we can get the same response by using function \( f \) and \( g \) with different \( C_{RO} \) and \( S \). Function \( f \) and \( g \) are independent. The function \( f \) is to rearrange the column vectors, and the function \( g \) is to select the column vector elements. In the one-to-many authentication, \( f \) and \( g \) are used for the configuration to get the same response from any two different CRO PUFs. Based on this, we can design a shared pairing key generation scheme. In what follows, we give an example to explain the idea.

Taking two CRO PUFs as an example, each CRO PUF contains four 4-layer inverters. The corresponding delay models are represented by matrices \( A \) and \( B \), respectively.

\[
A = \begin{bmatrix}
3 & 6 & 8 & 5 \\
2 & 4 & 6 & 5 \\
9 & 7 & 4 & 5 \\
5 & 4 & 6 & 5
\end{bmatrix}
B = \begin{bmatrix}
1 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
5 & 6 & 3 & 3 \\
2 & 5 & 6 & 3
\end{bmatrix}
\]

Consider the following challenges:

\[
C_A = \{\{1,2\}, \{2,3\}, \{3,4\}\}
C_B = \{\{1,3\}, \{3,4\}, \{4,2\}\}
\]

In this case, the responses of both CRO PUFs are \( \{0,1,1\} \). Similarly, assuming the challenges are

\[
C_A = \{\{4,2\}, \{2,3\}, \{3,1\}\}
C_B = \{\{1,2\}, \{2,4\}, \{4,3\}\}
\]

Keep the selection signals \( S \) in \( A \) unchanged and adjust \( S_2 \) and \( S_4 \) in \( B \), the path delay models become

\[
A = \begin{bmatrix}
3 & 6 & 8 & 5 \\
2 & 4 & 6 & 5 \\
9 & 7 & 4 & 5 \\
5 & 4 & 6 & 5
\end{bmatrix}
B = \begin{bmatrix}
8 & 1 & 5 & 5 \\
3 & 6 & 4 & 2
\end{bmatrix}
\]

The delays of \( A \) and \( B \) become

\[
D_A = \{22, 25, 20, 16\}
D_B = \{17, 21, 19, 15\}
\]

In this case, the responses of both CRO PUFs are \( \{0,1,0\} \).

B. Modeling of Delay Matrix

We used machine leaning algorithms to model the CRO PUF and get the required delay matrix. The real delay matrix of the PUF that is implemented on hardware is called the original delay matrix, and the delay matrix we obtained through modeling is called the predicted delay matrix.

In the real scenario, it is difficult to get the original delay matrix, but all delay paths and their corresponding numbers in the counters can be measured on the CRO PUF. Therefore, the predicted delay matrix can be generated with the following two steps:
1) Enumerate all delay paths and get the numbers in the counters on the original delay matrix.  
2) Build a model to obtain the predicted delay matrix. 

Generally, the PUF responses are generated with the challenges that are used to select any two delay paths to compare. For example, as shown in Fig. 6, the delay difference between the two paths (marked as red and blue) is \((a_1 + d_2 + c_3 + b_4 + a_5) - (c_1 + a_2 + d_3 + c_4 + c_5)\). However, in the actual model, the delay parameters are difficult to be predicted using original CRPs. Therefore, during the delay predicting phase, we use the numbers in the counters to compute the exact values of the delay of each configuration, named as Counts. For example, the configuration of the red path “\((a_1 + d_2 + c_3 + b_4 + a_5)\)” in Fig. 6 and the parameters of the delay matrix \(W\) can be shown as follows.

\[
C = \begin{bmatrix}
1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0
\end{bmatrix}, \quad W = \begin{bmatrix}
a_1 & a_2 & a_3 & a_4 & a_5 \\
b_1 & b_2 & b_3 & b_4 & b_5 \\
c_1 & c_2 & c_3 & c_4 & c_5 \\
d_1 & d_2 & d_3 & d_4 & d_5
\end{bmatrix}
\]

\(C \cdot W\) is the dot product of the matrix \(C\) and \(W\), so the number Counts in the counter given by:

\[
Counts = \frac{1}{C \cdot W}
\]  

All delay paths and their corresponding numbers in the counters can be enumerated for a CRO PUF. Therefore, machine learning algorithms can be used to fit the parameter \(W\) to get the predicted delay matrix of CRO PUF. In this case, the input-output behavior of CRO PUF is completely consistent with the predicted model.

Note that there is a counter access interface implemented by fuses in the PUF so that the designer can obtain the numbers in the counters to model the PUF, and then burn the fuses to destroy the access interface before distributing the chips for usage [33]. In this way, designers can model the PUF while attackers are prohibited.

C. Shared-key Generation

1) Reliable response Generation for Shared-key: Shared-key generation requires CRO PUF generating stable responses. As discussed above, we can get a high accuracy predicted delay matrix already. Therefore, the delay difference between any two paths can be obtained easily. On this basis, we sort the absolute values of the delay differences between all the paths by descending order, and take into account the influence of different temperatures to determine a threshold \(T\). When the absolute value of the delay difference between the two paths is greater than the threshold, the response of the two paths can be considered stable even under different temperatures. The selection of threshold shows as the Algorithm 1. In this algorithm, we store the absolute value of delay difference and configuration challenge between all paths in the set \(B\). Then we sort the elements in \(B\) by descending order according to the absolute value of delay difference. Finally, we enumerate the elements in \(B\) to determine whether the configuration challenge can generate stable response at different temperatures. If a configuration challenge does not produce a stable response, we will use the absolute value of the delay difference between the two paths as the threshold \(T\), and the threshold would be increased to ensure that a stable response is generated. The detailed explanation for Algorithm 1 is as follows.

- Store all paths of delay matrix \(A\) into the set \(D\) (line 3);
- Enumerate all combinations of two different paths in the set \(D\) (line 4-7);
- Store the absolute value of the delay difference, configuration and challenge of two paths into the set \(B\) as an element (line 5);
- Sort the elements in the set \(B\) by descending order according to the absolute value of delay difference (line 8);
- Enumerate the elements in the set \(B\) and determine whether the response generated by the corresponding configuration and challenge keeps stable at different temperatures (line 11-18);
- If stable, continue to enumerate the elements in the set \(B\). Otherwise, use the absolute value of the current delay difference as the appropriate threshold \(T\) and end

![Fig. 6. An example of two delay paths](image)
Algorithm 2: Challenge generation

1. input: Delay matrix $A$, Threshold $T$, Shared-key $K$
2. output: Challenge $C$
3. Initialize: $D$: the set of all possible path delay in $A$
4. $N = \text{Size}(K)$
5. for $i = 1, 2, ..., N$ do
6.   while $d_1 \leftarrow \text{random}(D)$, $d_2 \leftarrow \text{random}(D)$ and Path($d_1$) ≠ Path($d_2$) do
7.     // random($D$): select a random path delay in $D$
8.     if $K_i = 1$ and $d_1 \cdot d_2 > T$ then // $K_i$ is the $i$-th bit of $K$
9.       $C_i = \text{Config}(d_1, d_2)$ // $C_i$ can generate $K_i$
10.      break
11.   end if
12.   else if $K_i = 0$ and $d_1 \cdot d_2 < T$ then
13.      $C_i = \text{Config}(d_1, d_2)$
14.      break
15.   end if
16. end while
17. end for
18. $C = \{C_1, C_2, ..., C_N\}$
19. return $C$

the loop. Note that, in practice, the threshold will be increased slightly to ensure response 100% reliable (line 14-16).

2) Challenge Generation for Shared-key: In the key-sharing protocol which we will introduce in the next section, a trusted third party (TTP) possesses the delay matrix of CRO PUF and the threshold for generating a stable response. The TTP needs to generate the challenges of CRO PUFs corresponding to the key that needs to be shared. In this Section, we propose a heuristic challenge generation algorithm shown in Algorithm 2. In the Algorithm 2, for each bit of the key, the TTP will randomly select two paths and determines whether their delay differences are greater than the threshold. If Yes, TTP will get configuration challenge for these two paths, otherwise TTP would reselect another two paths randomly to compute the challenge. The detailed explanation for Algorithm 2 is as follows.

- Store all paths of delay matrix $A$ into the set $D$ (line 3);
- Enumerate all the bits of the shared-key $K$ (line 4-17);
- Randomly select two different paths from the set $D$ (line 6-16);
- For each bit of the shared key $K_i$, if $K_i$ equals 1 and the delay difference is greater than $T$, it means that we found a configuration challenge $C_i$ that can generate a stable response 1 (line 8-10); If $K_i$ equals 0 and the delay difference is less than $-T$, it means that we found a configuration challenge $C_i$ that can generate a stable response 0 (code line 12-14); Otherwise, return to step 2.
- The configuration challenge $C$ is composed of all $C_i$ (line 18).

V. Security Analysis

The most important feature for physical unclonable function is "unclonable" obviously. However, this feature is threatened with the attack techniques reported recently. Machine leaning (ML)-based modeling attacks and side-channel attacks are two kinds of main threatens for RO PUF.

D. Key-sharing Protocol

As discussed above, CRO PUF can generate the shared key with the flexible configuration of $S$ and $C$. Therefore, it can be used as authentication of multi-party communication for adjacent resource-constrained nodes. As shown in Fig. 7, we propose a CRO PUF-based key-sharing and secret information transmission protocol.

Assuming that $PUF_A$ and $PUF_B$ require sharing the key. First, we send the delay matrix of $PUF_A$ and $PUF_B$ to the TTP, and in this case, the TTP carries the delay matrix of $PUF_A$ and $PUF_B$. Second, the TTP selects a key $K$ that needs to be shared between $PUF_A$ and $PUF_B$. Third, TTP generates the challenge $C_A$ and $C_B$ according to the delay matrix of $PUF_A$, $PUF_B$ and the shared-key $K$. Then TTP sends $C_A$ and $C_B$ to $PUF_A$ and $PUF_B$, respectively. Finally, $PUF_A$ and $PUF_B$ are able to generate the shared-key $K$ with $C_A$ and $C_B$, respectively. In the whole process, there is no secret key transmission. Besides, configuration information $S$ is not the secret information and can be stored in SRAM. Therefore, it is with high security and low cost to realize the key-sharing among multi-parties.

After $PUF_A$ and $PUF_B$ have obtained the shared-key, they can transfer the secret message to each other. For example, we suppose that Alice needs to send message $M(10100101)$ to Bob. At this time, Alice encrypts the message $M$ by XOR with the secret key $K(01101001)$ to generate the encrypted message $M'(11001100 = K \oplus M)$, and sends $M'$ to Bob. After receiving the $M'$, Bob gets the message $M(10100101 = M' \oplus K)$ by XOR with the secret key $K$.

As discussed above, a CRO PUF-based key-sharing method and the corresponding secure information transmission protocol are proposed. It is noted that PUF-based key-sharing is not specially designed for RO PUF but also can be applied to other PUF structures, provided that the delay information are obtained by testing and appropriate challenges are selected.
A. Modeling attacks

ML-based modeling attacks are the most efficient attack for strong PUFs which have a publicly accessible CRP interface so that attackers can collect a large number of CRPs to model the PUF with the mathematical way [1]. For example, our recent experimental results show that machine learning can foresee arbiter PUF responses to given 1000 CRPs with prediction rates up to 99%. However, crossover RO PUF is used as the weak PUF instead of strong PUF. The corresponding responses are used as keys. In such application, there is no access interface to read the key generated inside the chip so that the key will not be exposed to attackers (CRP access interface is implemented by fuses which will be destroyed after designers obtain the CRPs [33]). Therefore, CRO PUF is immune to ML-based modeling attacks.

B. Side-channel attacks

Side-channel attacks statistically analyze the time, power consumption or electromagnetic emanation of the cryptographic devices to gain knowledge about integrated secrets. Most recently, Merli et al. carried out side channel attacks (EM analyses) on an RO PUF FPGA implementation leading to the extraction of a full PUF model and thereby breaking the PUFs security [17]. The authors also point that their proposed attack can be successful because they exploit that each RO has a fixed location and a specific measurement path through a multiplexer to a counter. In this paper, we can dynamically change the inverters of ROs with different configuration data to generate the updated key, which makes each RO have no fixed physical location and therefore our proposed crossover RO potentially provides a new solution to resist side channel attacks. Moreover, the security can be enhanced by increasing the number of inverters in ROs and levels of ROs.

C. Cloning detection

In addition to resist cloning attacks, detecting simple clone is also feasible for CRO PUF. In [32], we illustrated a simple cloning scenario as follows.

Cloning Scenario: There are two RO pairs (A, B and C, D) with 5 inverters in each, generating two bits ‘01’. This means delay \( A > \) delay \( B \), and delay \( C < \) delay \( D \). The attackers can use the EM emanation to measure these two relations. To clone this PUF, they can simply build \( A \) and \( D \) with 5 inverters and build \( B \) and \( C \) with 1 inverter. The mismatching of inverter numbers will guarantee the cloned PUF generates the same response with the original one.

The traditional RO PUF is unable to detect the above cloning scenario. However, this potential clone can be detected with the help of configuration vectors of our proposed configurable RO PUF. In what follows, an authentication-based cloning detection method is proposed to determine whether CRO PUF is cloned or not.

The idea is alternated by authentication process. Besides the secret key configuration vector \( V_k \), we introduce the testing vector \( V_t \) for anti-cloning purpose. Testing vector \( V_t \) is carefully selected to generate stable testing response \( R_{th} \). In the working phase, \( V_k \) is configured to PUF to obtain the reliable secret key. In detecting phase, \( V_t \) is configured to PUF to achieve the test bitstream \( R_{th} \). For cloning detection, we can use multiple testing vectors. All these vectors should be very different with each other. It is better to cover all the inverters during the testing phase. In the cloning scenario, it could possibly provide the same response under a specific configuration vector. However, when several configuration vectors are used, the probability of generating the right responses decreases dramatically.

The rationale of above approach is that configurable RO can be used to generate CRPs. The configuration vector is the challenge. The famous 1-out-of-8 RO PUF and [10] provide the challenge and response schematics, respectively. But the sizes of their challenges are not large enough for authentication. Configurable RO PUF can provide enough CRPs with adequate length of each RO. Even though configurable RO PUF can be used in authentication field, we do not suggest it to be a conventional authentication PUF, like arbiter PUF. People should not get unlimited access of \( V_t \), otherwise it will suffer from modeling attacks. A few carefully selected configuration vectors are enough to reduce the cloning risk [32].

In addition to the above discussed cloning scenario, there would be other cloning scenarios, and the corresponding countermeasures also need to be developed. We call for more comprehensive researches on this topic.

VI. EXPERIMENTAL RESULTS

The experiments to evaluate the effectiveness of crossover RO PUF are conducted based on the public PUF dataset of Virginia Tech [18]. This dataset consists of frequency of ROs from 198 Xilinx Spartan (XC3S500E) FPGA boards. Since this dataset only has the frequency of ROs without individual inverters, we can treat each RO as an inverter in our experimentation due to the lack of public data on delay at inverter level.

Among the 198 boards, 194 boards measure the frequencies of ROs at the temperature 25°C and the supply voltage of 1.20V. The other five boards measure the frequencies at varying supply temperatures and voltages. The ranges of temperatures are 25°C, 35°C, 45°C, 55°C and 65°C. The supply voltages are 0.96V, 1.08V, 1.20V, 1.32V and 1.44V. We use the frequency dataset from five boards (D059546, D113702, D113938, D225158 and D225159) to compare the hardware efficiency, uniqueness and reliability for traditional neighbor coding method, rPUF in [14], and our proposed crossover RO PUF, respectively.

A. Hardware Efficiency

The total number of configurations is determined by the number of inverters in ROs and levels of ROs in the crossover RO PUF structure. There are \( (A^n_m)^{m-2} \) configurations in \( n \) ROs when each RO has \( m \) (\( m \) must be odd and \( m > 2 \)) level inverters. For the rPUF [11] which has \( n \) ROs and \( m \) levels of inverters, the number of possible different configurations of the delay loops is \( \sum_{i=0}^{m-1} (C_{m+1}^{2i+1})^n \), where \( i = 0, 1, \ldots, \frac{m-1}{2} \). As shown in TABLE II and TABLE II when the number of
TABLE I
NUMBER OF CONFIGURATIONS FOR CROSSOVER RO PUF.

| m | n = 2 | n = 4 | n = 6 | n = 8 |
|---|------|------|------|------|
| 3 | 2    | 24   | 720  | 40320|
| 5 | 8    | 13824| 1.73E+08 | 6.55E+13|
| 7 | 32   | 7.96E+06 | 1.93E+14 | 1.07E+23|
| 9 | 128  | 4.59E+09 | 1.93E+14 | 1.73E+32|

TABLE II
NUMBER OF CONFIGURATIONS FOR rPUF [11]

| m | n = 2 | n = 4 | n = 6 | n = 8 |
|---|------|------|------|------|
| 3 | 1    | 1    | 1    | 1    |
| 5 | 101  | 10001| 1.00E+06 | 1.00E+08|
| 7 | 1667 | 1.69E+06 | 1.92E+09 | 2.29E+12|
| 9 | 24229| 3.04E+08 | 4.35E+12 | 6.60E+16|

TABLE III
HARDWARE OVERHEAD OF THE LOGIC ELEMENTS IN THE DESIGN

| Logic Element             | Overhead in terms of NAND gates |
|---------------------------|---------------------------------|
| 5-stage ring oscillator   | 5                               |
| 2-to-1 MUX                | 9                               |
| 4-to-1 MUX                | 13                              |
| 8-to-1 MUX                | 21                              |
| 7-stage ripple counter    | 49                              |

ROs is 8 and the levels of each RO is 5, the total number of configurations of crossover RO PUF reaches 6.55E+13 which is 6.55E+5 times larger than rPUF. We can see from TABLE I that the total number of configurations grows exponentially with the increasing of \( m \) and \( n \), which provides a simple way to increase the PUF response bits.

The RO PUF usually consists of some basic components such as ROs, multiplexers, counters, comparators and so on. We can calculate the total overhead of each RO PUF with the overhead of components in TABLE III. For example, decouple neighbor coding uses 512 ROs to form 256 RO pairs to generate 256-bit response; the overhead is \( 256 \times 2 \times 5 + 2 \times 49 = 27648 \). For a rPUF with 14 5-level ROs, the overhead is \( 14 \times (2 \times 5 + 2 \times 5 + 9 + 2 \times 49) = 2772 \). For a crossover RO PUF with 4 5-level ROs, the overhead is \( 4 \times 5 + 4 \times 13 \times 4 + 2 \times (49 + 13) = 352 \).

In order to evaluate the hardware efficiency of our proposed CRO PUF, we define the reliability threshold factor [15] which is denoted as \( \sigma \). Consider a pair of ring oscillator, \( RO_A \) and \( RO_B \), and assume their frequencies are \( F_A \) and \( F_B \), respectively. Then \( |F_A - F_B| \geq F_{TH} = F_{ref} \sigma \), where \( F_{ref} \) is the frequency of reference RO, and \( \sigma \) is the reliability threshold factor [15].

We use the bits per NAND gate to evaluate the hardware overhead of each RO PUF. Fig. 8 denotes the comparison of hardware efficiency of three methods. The hardware efficiency is denoted by the number of bits generated by per NAND gate. As shown in Fig. 8 more hardware resource would be used when the criterion on reliability threshold factor for acquiring reliable ones is tightened, and crossover RO PUF is obviously more efficient than the other two methods. For example, when \( \sigma \) is set to 0.01, compared with decouple neighbor coding and rPUF, CRO PUF can get 9.29 times and 1.26 times hardware reduction, respectively, when generating the same number of PUF response bits.

B. Uniqueness

The uniqueness shows that different chips will have distinct PUF outputs when fed with the same challenge. If the output information of PUF is used for uniquely identifying the chip, it is unacceptable that different PUFs produce the same or similar responses. Average Hamming distance (HD) is used to evaluate the uniqueness of PUF responses. For \( k \) L-bit PUF responses: \( P_1, P_2, \ldots, P_k \), the average HD is calculated as follows.

\[
u = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{HD(P_i, P_j)}{L} \times 100\%	ag{2}\]

where \( HD(P_i, P_j) \) denotes the HD between \( P_i \) and \( P_j \):

\[
HD(P_i, P_j) = \sum_{m=1}^{L} (r_{i,m} \oplus r_{j,m})
\]

where \( r_{i,m} \) and \( r_{j,m} \) are the \( m \)-th bit of \( L \)-bit \( P_i \) and \( P_j \), respectively.
TABLE IV
AVERAGE HD WITH FIVE BOARDS AT U=1.20V

| Method        | 25°C | 35°C | 45°C | 55°C | 65°C |
|---------------|------|------|------|------|------|
| Neighbor      | 0.467| 0.466| 0.465| 0.464| 0.461|
| rPUF          | 0.467| 0.469| 0.468| 0.463| 0.462|
| Crossover RO  | 0.490| 0.491| 0.492| 0.493| 0.492|

TABLE V
AVERAGE HD WITH FIVE BOARDS AT T=25°C

| Method   | 0.96V | 1.08V | 1.20V | 1.32V | 1.44V |
|----------|-------|-------|-------|-------|-------|
| Neighbor | 0.459 | 0.462 | 0.467 | 0.473 | 0.473 |
| rPUF     | 0.450 | 0.455 | 0.467 | 0.472 | 0.471 |
| Crossover RO | 0.500 | 0.491 | 0.490 | 0.499 | 0.492 |

Fig. 10. HD of crossover PUF output bits with temperature variation at U=1.20V

In the experiments, we extract a hundred of 256-bit outputs in each of five boards under 25°C and 1.20V. Fig. 9 shows the histogram of the inter-chip HD. The average HD between any two pairs was 125.4 (49.0%), which is relatively close to the ideal value 50%.

We get the PUF outputs at different temperature and voltage levels. TABLE IV gives the average HD in different temperatures with U = 1.20V. TABLE V shows the average HD in different voltages with T = 25°C. We can see from Fig. 9, TABLE IV and TABLE V that our proposed crossover RO PUF has high uniqueness.

C. Reliability
Reliability is used to measure the stability of PUF response in various environments. Ideally, the difference between any two responses generated by a PUF under the same challenge in repeated experiments should remain the same. Since factors such as ambient temperature variation and supply voltage fluctuation affect circuit delay in practice, the PUF responses may be unreliable. The following formula is used to evaluate the reliability of PUFs [1]:

\[ r = 1 - \frac{1}{x} \sum_{y=1}^{x} \frac{H D(R_i, R_{i,y})}{L} \times 100\% \] (4)

where \( x \) is the number of samples for PUF response; \( R_i \) is the response extracted from the board \( i \); \( L \) is the number of generated response bits by the PUF; and \( H D(R_i, R_{i,y}) \) denotes the HD between the response \( R_i \) and the \( y \)-th sampling \( R_{i,y} \).

The temperature variation plays a very important role to the PUF performance in normal usage scenarios, because it is an effective factor to affect the circuit delay. In this paper, we select the temperature and voltage as the effective environmental factors to verify the PUF performance.

For each 256-bit PUF on each board, we computed the HD between responses at various temperatures and voltages. As shown in Fig. 10, 92% of the responses were changed by ten or fewer bits when the range of temperature is 35°C to 65°C, and no response experienced more than 20 bit flips. The average is 3.33 (1.30% of the total number of 256 bits). More details of comparison under different temperatures are reported in TABLE VI. Comparing the Fig. 9 with Fig. 10, we can see a large gap in the distributions roughly between 21 ~ 90 bits, which demonstrates that our proposed CRO PUF can be effective for device authentication and anti-counterfeiting.

As shown in Fig. 11, the average distance between any two pairs under the range of voltages is quite similar to that of Fig. 10. The average HD increases from 3.33 to 3.61, and the maximum HD from 12 to 18. TABLE VII shows the comparison of average HD with various voltages for three methods. Comparing TABLE VII with TABLE VI we can see that the voltage factor has bigger influence on the PUF reliability than the temperature. However, comparing Fig. 11 with Fig. 10 we can see that the gap still exists in...
the distributions between 21 ~ 90 bits, which means the PUF proposed in the paper can still work effectively. As shown in TABLE VI and TABLE VII CRO PUF has a better reliability than the other two methods in tolerating the temperature and voltage variation.

Fig. 12 gives the reliability trend of RO PUF with various temperatures (25°C to 65°C) when the voltage U = 1.20V. It is shown that our proposed CRO PUF has better reliability with the factor σ increasing.

D. Key-sharing

1) Extracting of delay matrix: We extract the delay matrix for CRO PUFs with different sizes using the machine learning. The experiment is conducted on an Intel (R) Core i5-3230M CPU. We have extracted the delay matrices of different CRO PUF sizes such as 3 × 5, 3× 3, 3 × 9, 4 × 5, 4 × 7, 5 × 5, 6 × 7, and 7 × 5. In our experiments, all delay paths and the corresponding numbers in the counters are used as the training data, and all CRPs are used as the testing data. TABLE VIII gives the training time and the accuracy of the delay matrix extracted from CRO PUFs with different sizes. The accuracy is computed by comparing the matching rate of all CRPs generated on the original delay matrix and predicted delay matrix. Experimental results show that the predicted delay matrix can achieve 99.9% accuracy. We extracted the delay matrix from a 4 × 5 CRO PUF spending only 0.411s with 99.9% accuracy. For the 3 × 5 CRO PUF, we increased the training time to 5.096s to achieve 100% accuracy.

2) Coefficient of stabilization: In order to verify the usability of CRO PUF-based key-sharing method, we need to know how many reliable CRPs for a PUF with a specified appropriate threshold. In the experiment, we define the coefficient of stabilization (COS) to evaluate the percentage of reliable CRPs.

\[
COS = R_t / R
\]  

where \(R_t\) is the number of CRPs that satisfy the threshold condition, and \(R\) denotes the total number of CRPs.

The COS determines the number of reliable CRPs generated by the predicted delay matrix that we extracted. In the experiment, we computed the COSs of 100,000 simulated 4 × 5 CRO PUFs in three FPGA chips (D059546, D113702, D225159). The experimental results are shown in Fig. 13. The ordinate represents the number of CRO PUFs, and the abscissa represents the COS. For example, [41:50] means that the COS is between 41% and 50%. For a 4 × 5 CRO PUF, 10,368 different CRPs can be generated. Assuming that the COS of this CRO PUF is 50%, there are still 5184 CRPs that are reliable at different temperatures. As a weak PUF, CRO PUF can generate at least 100 reliable CRPs even with COS = 1%. We can see from Fig. 13 that very few COSs are located in the range of 3% ~ 50% in our experiments, which indicates that available CRPs are enough for key-sharing.

VII. CONCLUSION

In many embedded systems and IoT applications, resource-limited devices cannot afford the classic cryptographic security solutions. Lightweight security primitives are required. PUF is an alternative solution for low cost key generation. In this paper, we propose a new RO PUF structure which can effectively improve the reliability and increase hardware efficiency. By selecting different inverters in ROs, the frequency difference between two ROs will be larger than the threshold, and hence generate reliable responses. Compared to the previous configurable RO PUFs, the experiment results on the public
PUF dataset show that our proposed crossover RO PUF has higher reliability and hardware efficiency. This is also the first PUF structure that can generate the same shared-key in physically for all devices. Therefore, CRO PUF can be applied in the lightweight key-sharing protocol for IoT devices.

REFERENCES

[1] J. Zhang, G. Qu, Y. Lv, and Q. Zhou, “A survey on silicon pufs and recent advances in ring oscillator pufs,” Journal of Computer Science and Technology, vol. 29, no. 4, pp. 664–678, 2014.

[2] G. Hammouri, E. ztrk, and B. Sunar, “A tamper-proof and lightweight authentication scheme,” Pervasive and Mobile Computing, vol. 4, no. 6, pp. 807–818, 2008.

[3] S. S. Kumar, J. Guajardo, R. Maes, G. J. Schrijen, and P. Tuyls, “Extended abstract: The butterfly puf protecting ip on every fpga,” in IEEE International Workshop on Hardware-Oriented Security and Trust, 2008, pp. 67–70.

[4] J. H. Anderson, “A puf design for secure fpga-based embedded systems,” in Asia South Pacific Design Automation Conference, Taipei, Taiwan, January, 2010, pp. 1–6.

[5] J. Zhang, Q. Wu, Y. Lyu, Q. Zhou, Y. Cai, Y. Lin, G. Qu, “Design and Implementation of a Delay-Based PUF for FPGA IP Protection,” in International Conference on Computer-Aided Design and Computer Graphics, 2013, pp. 107-114.

[6] J. Zhang, Q. Wu, Y. Ding et al, “Techniques for Design and Implementation of an FPGA-Specific Physical Unclonable Function,” J. Comput. Sci. Technol., vol. 31, no. 1, pp. 124–136, Jan. 2016.

[7] Z. Liu, J. W. Lee, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas, “Extracting secret keys from integrated circuits,” IEEE Transactions on Very Large Scale Integration Systems, vol. 13, no. 10, pp. 1200–1205, 2005.

[8] G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” in Proceedings of the 44th annual Design Automation Conference, 2007, pp. 9–14.

[9] M. S. Kim, D. I. Moon, S. K. Yoo, and S. H. Lee, “Investigation of physically unclonable functions using flash memory for integrated circuit authentication,” IEEE Transactions on Nanotechnology, vol. 14, no. 2, pp. 384–389, 2015.

[10] 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.

[11] J. Zhang, Y. Lin, and G. Qu, “Reconfigurable binding against fpga replay attacks,” ACM Transactions on Design Automation of Electronic Systems, vol. 20, no. 2, pp. 1–20, 2015.

[12] M. Majzoobi, F. Koushanfar, and M. Potkonjak, “Techniques for design and implementation of secure reconfigurable pufs,” ACM Transactions on Reconfigurable Technology and Systems, vol. 2, no. 1, pp. 1–33, 2009.

[13] Y. Lao and K. K. Parhi, “Statistical analysis of mux-based physical unclonable functions,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 33, no. 5, pp. 649–662, 2014.

[14] M. Gao, K. Lai, and G. Qu, “A highly flexible ring oscillator puf,” in 2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC), 2014, pp. 1–6.

[15] B. Tang, Y. Lin, and J. Zhang, “Improving the reliability of ro puf using frequency offset,” in 13th International Conference on Field Programmable Technology, 2014, pp. 338–341.

[16] M. Majzoobi, F. Koushanfar, and S. Devadas, “Fpga puf using programmable delay lines,” in 2010 IEEE Workshop on Information Forensics and Security, 2010, pp. 1–6.

[17] D. Merli, J. Heyszl, B. Heinz, D. Schuster, F. Stumpf, and G. Sigl, “Localized electromagnetic analysis of ro pufs,” in IEEE International Symposium on Hardware-Oriented Security and Trust, 2013, pp. 19–24.

[18] A. Maiti and P. Schaumont, “Research on physical unclonable functions (pufs) at ses lab,” Virginia Tech, 2011.

[19] M. Majzoobi, “Reliable and efficient PUF-based key generation using pattern matching”, in IEEE Int. Symp. Hardware-Oriented Security and Trust (HOST), 2011, pp. 128-133.

[20] C. Yin and G. Qu, “Temperature-aware cooperative ring oscillator PUF,” in IEEE International Workshop on Hardware-Oriented Security and Trust, 2009, pp. 36–42.

[21] M. Majzoobi, M. Rostami, F. Koushanfar, D.S. Wallach, S. Devadas, “Slender PUF Protocol: A Lightweight, Robust, and Secure Authentication by Substring Matching”, in IEEE Sym. Security and Privacy Workshops (SWP), 2012, pp. 33-44.

[22] R. Maes, A. Van Hereweghe, and I. Verbauwhede, “PUFKY: A Fully Functional PUF-based Cryptographic Key Generator,” In Cryptographic Hardware and Embedded Systems (CHES), pp. 302-319, 2012.

[23] F. Koushanfar, “Provably Secure Active IC Metering Techniques for Piracy Avoidance and Digital Rights Management,” IEEE Trans. Information Forensics and Security, vol. 7, no. 1, pp. 51-63, Feb. 2012.

[24] Z. Pang, J. Zhang, Q. Zhou, S. Gong, X. Qian, and B. Tang, “Crossover Ring Oscillator PUF,” in Proceedings of the 18th International Symposium on Quality Electronic Design (ISQED), 2017, pp. 237C243.

[25] J. Zhang, Y. Lin, Y. Lyu, and G. Qu, “A PUF-FSM Binding Scheme for FPGA IP Protection and Pay-per-Device Licensing,” IEEE Transactions on Information Forensics and Security, vol.10, no.6, pp. 1137-1150, 2015.

[26] Y. Yang, L. Wu, G. Yin, “A Survey on Security and Privacy Issues in Internet-of-Things,” IEEE Internet of Things Journal, 2018.

[27] X. Xu and D. Holcomb, “A Clockless Sequential PUF with Autonomous Majority Voting,” in Proceedings of the 26th edition on Great Lakes Symposium on VLSI, 2016, pp. 27-32.

[28] J. Ye, Y. Hu, X. Li, “VPUF: Voter based Physical Unclonable Function with High Reliability and Modeling Attack Resistance,” in Proc. IEEE International On-Line Testing Symposium (IOLTS), 2017, pp. 74-79.

[29] “Ring Oscillator,” 2018. [Online]. Available: http://verayo.com/tech.php

[30] X. Xu and D. Holcomb, “HCIC: Hardware-assisted Control-flow Integrity Checking,” IEEE Internet of Things Journal, 2018.

[31] M. Gao, K. Lai, J. Zhang, G. Qu, A. Cui, and Q. Zhou, “Reliable and Anti-cloning PUFs Based on Configurable Ring Oscillators,” in Proc. the 14th International Conference on Computer-Aided Design and Computer Graphics (CAD/Graphics), 2015, pp. 194-201.

[32] C. Zhou, K. K. Parhi, and C. H. Kim, “Secure and Reliable XOR Arbiter PUF Design: An Experimental Study based on 1 Trillion Challenge Response Pair Measurements,” in Proceedings of the 54th Annual Design Automation Conference, 2017, pp. 1-6.

[33] L. Wei, C. Song, Y. Liu, J. Zhang, F. Yuan, and Q. Xu, “BoardPUF: Physical Unclonable Functions for printed circuit board authentication,” inProceedings of the IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2015, pp. 152-158.