A Dynamically Configurable PUF and Dynamic Matching Authentication Protocol

YALE WANG, CHENGHUA WANG, CHONGYAN GU, (Member, IEEE), YIJUN CUI, (Member, IEEE), and WEIQIANG LIU, (Senior Member, IEEE)

Yale Wang, Chenghua Wang, Yijun Cui and Weiqiang Liu are with College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics (NUAA), Nanjing 211106, China.

Chongyan Gu and Maire O’Neill are with the Centre for Secure Information Technologies (CSIT), Institute of Electronics, Communications & Information Technology (ECIT), Queen’s University Belfast (QUB), BT3 9DT, Belfast U.K.

ABSTRACT A physical unclonable function (PUF) is a hardware security primitive, which can be used to securely gover various hardware-based applications. As a type of PUFs, strong PUFs have a large number of challenge-response pairs (CRPs), which can be used for authentication. Present, most strong PUF structures follow a one-to-one input/output relationship, i.e., linear function. As such, strong PUF designs are vulnerable to machine learning (ML) based modeling attacks. To address the issue, a dynamically configurable PUF structure is proposed in this article. A mathematical model of the proposed dynamic PUF is presented and the design is proposed against the effective ML based attacks, such as deep neural network (DNN), logistic regression (LR) and reliability-based covariance matrix adaptation evolution strategies (CMA-ES). Experimental results on field programmable gate arrays (FPGAs) show that the proposed dynamic structure has achieved good uniqueness and reliability. It is also shown that the dynamic PUF has a strong resistance to the CMA-ES attack. Due to the dynamic nature of the proposed PUF structure, an authentication protocol is also designed to generate recognizable authentication bits string. The protocol shows strong resistance to classical machine learning attacks including the new variant of CMA-ES.

INDEX TERMS Physical unclonable function, dynamically configurable, machine learning, authentication protocol

I. INTRODUCTION The Internet of Things (IoT) has been widely deployed and will impact many applications in the near future. IoT which comprise huge heterogeneous networks can connect billions of devices. Unfortunately, this heterogeneity and connectivity of devices introduce significant security and privacy risks. The security of IoT will determine its widespread deployment and application [1].

Authentication mechanisms are used to prevent the unauthorized access to IoT devices. However, using traditional authentication approaches leads to a significant overhead for many lightweight IoT devices. Physical unclonable function (PUF), a lightweight hardware security primitive, can provide low-cost identity authentications for IoT devices [2], [3]. PUFs use the natural process variations of integrated circuits to create digital sequences, which are unique to each device. Depending on the quantity of CRPs, PUFs can be divided into weak PUFs and strong PUFs [4], [5]. Weak PUFs have a limited number of CRPs, which make them suitable for generating random sequences. PUFs do not need to store secrets in non-volatile memory (NVM) as other conventional cryptographic approaches. Strong PUFs having an exponential number of CRPs, are suitable for securing authentication protocols [6], [7]. However, most of the strong PUFs are vulnerable to ML based modeling attacks. In order to improve the security of strong PUFs, two approaches have been shown, one is introducing nonlinearity into the linear model of strong PUFs, such as the XOR arbiter PUF (XOR APUF) design. The other one is using reconfigurability to increase modeling attack resistance [9], [10]. Since the principle of ML modeling attacks is to model a PUF design from the static relationship between its challenges and responses, reconfigurable mechanisms can greatly improve the resistance of ML based modeling attacks [11]. However, in conventional reconfigurable...
designs, the reconfigurable signals are provided by inputs from outside, which achieve a limited improvement against ML attacks. Hence, changing the configurations of a PUF design dynamically and autonomously could be a promising way to improve the security of strong PUFs.

The dynamic mechanism provided in [12] reconfigured the PUF structure by loading different bitstream files, where the bitstream files contain different logic and routing constraints. However, recent studies have shown a successful attack on the Xilinx 7-series bitstream file [13]. In addition, the time cost of reloading a bitstream file on an FPGA is significant. It takes about 25 seconds to configure the PUF remotely, and in contrast, it only takes less than a millisecond to receive the PUF responses [12].

In this paper, we propose a dynamically configurable PUF structure, in which the configuration signal is independent of the inputs (challenges). A dynamic matching authentication protocol based on the dynamic PUF is also proposed. The main contributions of the paper can be summarized as follows:

- A dynamically configurable hybrid (DCH) PUF structure is proposed. Each response bit is generated once with one configuration. The configuration signals are generated from an internal linear feedback shift register (LFSR) and are independent from the inputs. The longer the bit-length of the LFSR, the larger the number of configurations, and the greater the computational cost of a modeling attack.
- DNN, LR and reliability-based CMA-ES algorithms, the most effective modeling attacks against n-XOR APUFs designs, are utilised to analyze the resistance capability of the proposed DCH PUF. The analysis shows that the proposed DCH PUF structure can resist these ML attacks due to its dynamic configuration features.
- An authentication protocol based on the proposed dynamic PUF is presented. The protocol uses pattern matching and has a strong error tolerance. The authenticating process without using the complete response shows great resistance to classical ML attacks and the latest variant of CMA-ES against pattern matching.

The rest of this paper is organized as follows. Section II introduces a background research related to this paper. In Section III, configurable PUF structures and their mathematical models are introduced. The proposed dynamically configurable PUF structure is also introduced. Section IV evaluates the response performance of the DCH PUF. Its security is comprehensively evaluated, and its performance against modeling attacks along with their cost is provided. Section V introduces the proposed authentication protocol based on the DCH PUF structure. Section VI evaluates the security performance of the proposed authentication protocol. A discussion and conclusion are given in Section VII.

II. RELATED WORK

A. PUF DESIGNS AND ATTACKS

Various PUF designs and attacks have been studied over the past decade. Arbiter PUF (APUF) designs generate responses via a race between the signals in two delay chains. However, due to the linear characteristics of its model, the original APUF structure can be easily modeled [8]. One proposal to improve its resistance to modeling attacks is to introduce nonlinearity. In feed-forward PUFs (FF-PUFs) [14], the challenges of some stages are determined by feed-forward branches. The cost of modeling FF PUF designs increases with the number of FF loops. XOR APUF designs [15] generate responses by XORing the responses of multiple individual APUFs. The cost (in terms of the number of CRPs required) of using a classic ML algorithm to attack this design increases exponentially with the number of individual APUFs used.

Building on the XOR APUF structure, the lightweight secure PUF [16] changed the sequence of individual APUF challenge bits, to further increase the resistance to ML attacks. Based on the lightweight secure PUF, TSMA PUF [17] uses multiplexers to choose different path combinations before the arbiters of two individual APUFs. The more recently proposed interpose PUF structure [18] comprises two XOR APUFs, where the response of the upper XOR APUF structure is used as one bit of the lower XOR APUF challenge and the response of the lower XOR APUF is taken as the final response. This design has stronger ML resistance than XOR APUFs of the same scale.

In terms of attacks against PUF designs, DNN, LR, and CMA-ES are the main methods used in recent studies. DNN-based attack [19] is a form of black box attacks and does not need a specific mathematical model. It can predict the PUF response by training the inner multilayer neurons. In [20], the authors successfully predicted the responses of a double arbiter PUF using DNNs. LR is a gradient descent ML algorithm, which can efficiently model XOR APUFs based on a special transformation of their mathematical model.

Although the CMA-ES algorithm [22] has a large search space and needs a long training time, its fitness function is not limited to a specific form. Therefore it has a wide range of applications and can be used to model all known strong PUF structures. The CRP based CMA-ES algorithm is less efficient than LR when attacking XOR APUFs [18], [23], but Becker [24] proposed a new reliability-based CMA-ES algorithm, which is more efficient than LR when attacking XOR APUFs with large numbers of individual APUFs. The amount of CRPs needed only increases linearly with the number of individual APUFs. Before that, the classical ML algorithms could only model XOR APUFs or lightweight secure PUF composed of a small number of individual APUFs. With the reliability-based CMA-ES algorithm, both the structures with more than 9 individual APUFs have been broken [24]. The interpose PUF has also been broken by a new divide-and-conquer approach [25].

B. PUF-BASED AUTHENTICATION PROTOCOLS

The majority of authentication protocols using PUFs are based on the static response behaviour of PUF structures [17], [26], [27], and therefore, are not suitable for the
proposed DCH PUF structure. In the proposed structure the
time-varying configuration ensures that the challenges and
responses do not have a one-to-one relationship. Therefore,
on the basis of the fixed order of different configurations, an
approach based on pattern matching is used to authenticate
the structure.

Another protocol based on pattern matching is the Slender
protocol [28]. In this protocol, only a random substring of
the real response is included in the authentication bits string,
and the remainder is made up of random padding. This
method greatly expands the attacker’s search space and
makes the traditional CRP-based ML attacks practically
invalid. However, Becker proposed a CMA-ES algorithm
based on a Hamming weight (HW) [29]. With this method,
the two random indexes used in the Slender protocol cannot
provide resistance and the protocol was broken by this
method at a relatively small cost.

C. MODEL OF AN ARBITER PUF

The APUF, a basic strong PUF structure, consists of two par-
allel n-stage multiplexer (MUX) chains and an arbiter. Dur-
ing operation, an enable signal activates the circuit. Two
parallel n-stage MUX chains feed into an arbiter (D flip-flop)
to produce one response bit. An n-bit challenge
\( \{c_0, c_1, c_2, \ldots, c_{n-1}\} \) determines whether the signal passes
through parallel or cross paths at the nth stage. When the sig-
als from two chains arrive at the arbiter, a decision will be
given depending on the arriving time. Finally, the arbiter out-
puts ‘0’ or ‘1’ according to which signal arrives first.

According to the working principle of an APUF, a model
of its response can be considered as an additive delay model
[24]. Therefore, the response \( R_{apuf} \) of an n-stage APUF can be represented as

\[
R_{apuf} = \begin{cases} 
0, & \Delta_{apuf}(n) > 0 \\
1, & \Delta_{apuf}(n) \leq 0 
\end{cases},
\]

where \( \Delta_{apuf} \) is the decision delay of an APUF, and
\[
\Delta_{apuf}(n) = \tilde{P} \cdot \tilde{W}^T,
\]

where \( \tilde{P} \) is the challenge parity vector, \( \tilde{P} = \{p_1, p_2, \ldots, p_n\} \).
Due to the APUF characteristics, each bit of the challenge
not only determines whether to choose the parallel or oppo-
site paths, but also affects the number of times that two com-
peting paths exchange signals before the two signals arrive at
the arbiter. Therefore, the challenge parity vector is calculated
by the value and position of each challenge bit. The challenge parity
\( p_k \in \{-1, 1\} \) is defined by
\[
p_k = \prod_{i=k+1}^{n} (1 - 2c_i),
\]
and \( \tilde{W} \) is the delay vector, \( \tilde{W} = \{\omega_1, \omega_2, \ldots, \omega_{n-1}\} \). The elements of \( \tilde{W} \) are dependent on the multiplexer switching
and routing delays, which are susceptible to manufacturing
process variations even if the switching of each APUF stage
is identically designed. The elements of the weight vector \( \tilde{W} \)
are given by
\[
\omega_1 = \alpha_1, \omega_i = \alpha_i + \beta_{i-1}, \text{for } 2 \leq i \leq n, \omega_{n+1} = \beta_{n-1},
\]

where \( \alpha_i \) and \( \beta_i \) can be calculated by
\[
\alpha_i = \frac{(q_i - r_i - s_i + t_i)}{2}, \beta_i = \frac{(q_i - r_i + s_i - t_i)}{2},
\]

where \( q_i, r_i, s_i \), and \( t_i \) represent the four path delays possible in the
ith stage of the two-MUX chain, as shown in Figure 1. Using this model, by collecting a certain number of CRPs to
train a ML algorithm, the unknown response of an APUF
can be effectively predicted [8].

D. PUF RESPONSE PERFORMANCE METRICS

Uniqueness. Ideally, no two chips should generate the same
responses. A Hamming distance (HD) is utilized to calculate
the difference between two responses. The ideal value of
uniqueness is 50 percent when the same challenge \( C \) is input.
When the same PUF circuit is implemented in the device \( i \)
and device \( j \), n-bit responses \( R_i \) and \( R_j \) will be generated.
The uniqueness can be expressed as the average inter-chip HD
over \( k \) devices, as follows:
\[
Uniqueness = \frac{2}{k(k-1)} \sum_{i=1}^{k} \sum_{j=i+1}^{k} HD(R_i, R_j) \frac{N}{N}.
\]

Reliability. The reliability of a PUF design reflects the abil-
ity to reproduce a response. The higher the reliability, the
lower the response error rate and the more stable the struc-
ture. In this work, the bit error rate (BER) is calculated as fol-
lows:
\[
BER = \frac{1}{s} \sum_{i=1}^{s} \frac{HD(R_i, R'_{ij})}{N},
\]

where \( s \) is the number of measurements, \( n \) is the bit-length of
the response, \( R_i \) is the reference response, and \( R'_{ij} \) is the
response of the ith measurement. The metric for reliability is
calculated as follows:

\[ \text{Reliability} = 1 - BER. \quad (8) \]

### III. THE PROPOSED DYNAMICALLY CONFIGURABLE PUF DESIGN

In this section, we first introduce two configurable PUF structures, and then show the proposed DCH PUF structure which is composed of these two structures and a dynamic configuration mechanism.

#### A. CONFIGURABLE SELF-XOR STRUCTURE

A configurable self-XOR (SX) structure is shown in Figure 2. Different from the traditional XOR APUF structure, the proposed self-XOR structure truncates the original APUF to generate multiple responses and then XORs them to derive a 1-bit final response. With this PUF structure there are many possible ways to choose the branch signal. A group of \((m+1):k\) MUXs is utilised to select different combinations, and the selected signals of the MUXs are called configuration signals. In addition, a ‘0’ signal is added to the signal options of MUX, which means that under a specific configuration signal, the structure is equivalent to a traditional APUF structure. It is worth noting that adding one branch requires only a small amount of additional resources (an arbiter, a MUX and an XOR gate). Compared with the traditional \(n\)-XOR APUF structure, this design can save a significant hardware resource.

Let \(R_{xx}\) represent the output of the configurable self-XOR structure. The response can be expressed as follows:

\[ R_{xx} = \begin{cases} 0, & \Delta_{sx}(n) > 0 \\ 1, & \Delta_{sx}(n) \leq 0 \end{cases}, \quad (9) \]

where \(\Delta_{sx}\) represents the delay difference of two signals fed into the self-XOR structure, which can be calculated as the product of the delay difference between the main circuit (APUF) and the branch circuit, as follows:

\[ \Delta_{sx}(n) = \Delta_{apuf}(n) \cdot \Delta_{bran}. \quad (10) \]

The branch delay difference \(\Delta_{bran}\) represents the delay difference of the selected branch, which is calculated by the configuration vector \(\vec{S}_{conf}\) and the delay difference vector \(\vec{\delta}_{bran}\) of multiple branches, as follows:

\[ \Delta_{bran} = \vec{\delta}_{bran} \cdot \vec{S}_{conf}^T = \prod_{i=1}^{k} \Delta_{apuf}(s_i), \quad (11) \]

where \(\vec{\delta}_{bran} = \{\Delta_{apuf}(s_1), \Delta_{apuf}(s_2), \ldots, \Delta_{apuf}(s_m)\}\) is the set of delay differences of all configurable branches, \(k\) is the number of selected branches, \(\Delta_{apuf}(s)\) represents the delay difference of an APUF with \(s\) stages, which can be calculated by Eq. (1). Note here that there is an extra ‘0’ signal in the design and when it is selected, the corresponding delay is \(\Delta_0 = 1\). The element \(s_i \in \{0,1\}\) in the configuration vector \(\vec{S}_{conf} = \{s_1, s_2, \ldots, s_m\}\) is defined by the configuration signals.

#### B. CONFIGURABLE MODIFIED FEED-FORWARD STRUCTURE

A configurable modified feed-forward (MFF) structure is proposed and shown in Figure 3, which differs from the original feed-forward APUF structure. In this structure, a MUX is added between the feed-forward signal and the target stage. The original challenge bit of the target stage provides the second input to the MUX. The selected signals are called configuration signals. Also, by using a certain configuration signal, the structure is equivalent to a traditional APUF structure. Let \(R_{mff}\) represent the output of the modified feed-forward structure, then

\[ R_{mff} = \begin{cases} 0, & \Delta_{mff}(n) > 0 \\ 1, & \Delta_{mff}(n) \leq 0 \end{cases}, \quad (12) \]

where \(\Delta_{mff}\) represents the delay difference of the modified feed-forward structure, which can be calculated from the challenge parity vector \(\vec{P}_{mff}\) and delay vector \(\vec{W}\),

\[ \Delta_{mff}(n) = \vec{P}_{mff} \cdot \vec{W}^T, \quad (13) \]

where \(\vec{P}_{mff} = \vec{P} \cdot \vec{S}_{conf}^T + \vec{P}_T \cdot (1 - \vec{S}_{conf})^T\), and \(\vec{P} = \{p_1, p_2, \ldots, p_n\}\) is the parity vector of the underlying APUF, and its elements \(p_k = \prod_{i=k+1}^{n} (1 - 2c_i)\). \(\vec{P}_T = \{p_{T_1}, p_{T_2}, \ldots, p_{T_j}\}\) is the set of all configurable FF loops, where the elements are...
The proposed APUF-based DCH structure.

The proposed 2-XOR-based DCH structure.

A Dynamically Configurable PUF and Dynamic Matching Authentication Protocol

\[ p_{r_1} = (1 - 2R_{apuf}(s_1)) \prod_{i=T_1+2}^{n} (1 - 2c_i), \]

\[ p_{r_2} = (1 - 2R_{apuf}(s_2)) \prod_{i=T_2+2}^{n} (1 - 2c_i), \]

\[ p_{r_j} = (1 - 2R_{apuf}(s_j)) \prod_{i=T_j+2}^{n} (1 - 2c_i). \]

(14)

The elements \( s_i \in \{0, 1\} \) in the configuration vector \( S_{bran} = \{s_1, s_2, \ldots, s_n\} \) can be transformed from the configuration bits, and \( R_{apuf}(s) \) represents the response of an APUF with \( s \) stages, which can be calculated from Eq. (1).

C. DYNAMICALLY CONFIGURABLE STRUCTURE DESIGN

Different structures can be formed from the above two structures with different configuration signals. Similar as existing work in [10], the configuration signals typically come from the challenge. Different from the way that the configuration signals of conventional configurable PUFs are provided by external inputs, in the proposed design, an internal LFSR provides the configuration signals. The LFSR does not require any seed from external inputs, and is driven by internal clock signal of the device. Its dynamic configuration signals are completely independent from external inputs. During the operation, the LFSR will jump to the next state when a response is generated. The configuration signal will change accordingly. This leads to different responses even if the same challenge is provided multiple times. Therefore, a dynamically configurable hybrid PUF structure which incorporates the dynamically configurable SX-PUF (DC SX-PUF) and the dynamically configurable FF-PUF (DC FF-PUF) is proposed.

Design Constraints. From the two configurable structures proposed above, there are many different configuration options for a multi-stage PUF structure. Previous work shows that the reliability of the XOR APUF and FF-PUF designs were reduced with an increased number of XORs and FF loops, respectively [9]. To mitigate the deterioration of reliability, the following constraints are proposed: 1) the number of branches that participate in an XOR operation in the configurable self-XOR structure is 1; 2) in the configurable FF structure, the number of FF loops is 2, and the two FF loops are overlapped. The response of the proposed DCH PUF is

\[ R_h = \begin{cases} 0, & \Delta_h(n) > 0 \\ 1, & \Delta_h(n) \leq 0 \end{cases}, \]

(15)

where

\[ \Delta_h(n) = \Delta_{sx}(n) \cdot \Delta_{mff}(n), \]

(16)

where \( \Delta_{sx}(n) \) and \( \Delta_{mff}(n) \) can be calculated from Eqs. (10) and (13), respectively. Note, due to the constraints of the proposed design, the self-XOR structure and the different FF loops in the hybrid structure will not affect each other and can be calculated separately. In addition, according to these constraints, a 64-stage APUF can provide up to 15 dynamic configuration bits. Figure 4 shows the APUF based DCH structure.

When the proposed DCH structure is applied to an XOR APUF or lightweight secure PUF structure, it is slightly different: only one of the SX branches containing the different PUFs is selected for input into the XOR operation by the configuration signal. In addition, in a multiple-XOR APUF based DCH PUF structure, only one LFSR is used to provide all the configuration signals. Figure 5 shows a 2-XOR APUF based DCH structure.

IV. ANALYSIS OF DCH PUF STRUCTURE

A. PERFORMANCE ANALYSIS

Uniqueness. First, a 7-bit APUF-based DCH structure was implemented on five Xilinx Artix-7 FPGA (28nm Technology) Nexys4 boards. Figure 6 shows the uniqueness results (average HD) of both the proposed DCH structure and its underlying APUF design. The uniqueness of the underlying APUF is only 11.8 percent, and the uniqueness of the 7-bit APUF-based DCH PUF is 41.0 percent. The improvement can be explained as follows. The proposed DCH PUF
configuration could be any of them, such that,

$$\text{BER}(\text{DCH}) = \sum_{i=1}^{2^n-1} \Pr(S_{\text{conf}} = S_i)\text{BER}(\text{CONF}_i)$$

$$= \frac{1}{2^n - 1} \sum_{i=1}^{2^n-1} \text{BER}(\text{CONF}_i),$$

where \(\text{CONF}_i\) represents one of the configurations provided by the LFSR.

**Reliability.** We tested the BERs of instances implemented on the FPGA boards, and compared them with \(n\)-XOR APUFs and \(n\)-stage FF APUFs, as shown in Table 1. For each structure, CRPs were collected 10 times using the same challenge set (contains 10,000 challenges). The APUF designs were implemented on the FPGA with fixed placement: only one LUT is selected in each slice to implement one MUX of the PUF delay chains, and all the slices are from one column. In Table 1, 1-SX APUF refers to the structure with one self-XOR branch. 2-FF APUF refers to the structure with two FF loops. 1-SX-2-FF APUF refers to the structure with one SX branch and two FF loops.

As \(n\) increases, the BER of DCH structure increases. However, when \(n\) is greater than 7, the BER begins to maintain at a certain level. More specifically, when \(n\) is greater than 7, the BER of the APUF-based DCH structure is equivalent to that of the 2-XOR APUF. In the traditional XOR structure, as the number of XOR gates increases, its reliability decreases sharply. With an increase in the bit-length of the configuration signal, the reliability of the DCH structure does not deteriorate significantly. The reason is that the proposed DCH structure is limited to at most one SX branch and two FF loops, and its BER is equivalent to the average BER of all these combination configurations.

**Hardware Consumption.** The original 64-stage APUF, implemented on FPGA with fixed placement, needs 129 slices, 128 for the 128 MUXs with 64 stages, and the last one for the arbiter. Compared with the APUF structure, the DCH PUF structure contains additional branches and a LFSR. Table 2 shows the numbers of slices required for the underlying \(n\)-XOR APUF the DCH structures. In fact, these branches and a small-scale LFSR can be implemented with few hardware resources. The implementation of the DCH structure

![Image 44x81 to 254x250]

**FIGURE 6.** Uniqueness of DCH PUF and its underlying APUF: (a) Uniqueness of underlying APUF; (b) Uniqueness of DCH PUF.

![Image 220x350]

**FIGURE 7.** Hamming distance of 128 configurations of a 7-bit DCH structure.

![Table 1](image)

**TABLE 1.** BER comparison (room temperature, normal supply voltage).

<table>
<thead>
<tr>
<th>PUF structures</th>
<th>BER</th>
<th>PUF structures</th>
<th>BER</th>
</tr>
</thead>
<tbody>
<tr>
<td>APUF</td>
<td>0.69%</td>
<td>3-bit DCH APUF</td>
<td>0.81%</td>
</tr>
<tr>
<td>2-XOR APUF</td>
<td>1.40%</td>
<td>4-bit DCH APUF</td>
<td>1.00%</td>
</tr>
<tr>
<td>3-XOR APUF</td>
<td>2.17%</td>
<td>5-bit DCH APUF</td>
<td>0.96%</td>
</tr>
<tr>
<td>4-XOR APUF</td>
<td>2.91%</td>
<td>6-bit DCH APUF</td>
<td>1.08%</td>
</tr>
<tr>
<td>1-SX-APUF</td>
<td>1.06%</td>
<td>7-bit DCH APUF</td>
<td>1.32%</td>
</tr>
<tr>
<td>2-FF-APUF</td>
<td>1.47%</td>
<td>8-bit DCH APUF</td>
<td>1.42%</td>
</tr>
<tr>
<td>1-SX-2-FF APUF</td>
<td>1.51%</td>
<td>9-bit DCH APUF</td>
<td>1.45%</td>
</tr>
<tr>
<td>4-bit DC SX-APUF</td>
<td>0.99%</td>
<td>10-bit DCH APUF</td>
<td>1.40%</td>
</tr>
<tr>
<td>6-bit DC FF-APUF</td>
<td>1.12%</td>
<td>11-bit DCH APUF</td>
<td>1.36%</td>
</tr>
</tbody>
</table>
only consumes a little more hardware than its underlying PUF. Taking the 9-bit DCH structure as an example, when the underlying structure is an original APUF, it only uses 13 more slices (3 for the 9-bit LFSR, 7 for the 7 branch arbiters, and 3 for the three 8:1 MUXs). Similarly, when the underlying structures are 2-XOR APUF and 3-XOR APUF, an additional 14 and 13 slices are needed, respectively. Since the proposed design is based on APUF or XOR APUF, and additional hardware consumption is needed for configuring the branches. Therefore, it will inevitably need more hardware resources than the underlying PUF structure. However, when increasing the number of branches, the number of hardware units required will not be multiplied as XOR APUF does.

### B. SECURITY ANALYSIS

In this subsection, we will show the resistance of the DCH PUF structure to modeling attacks. All the simulations in this work are performed on an Intel Xeon E5-2695 processor, 16 cores with 64GB are used for each run.

In the existing configurable PUF designs, the configuration signals are input from the outside of the device. This mechanism enables the device side to change the configuration on demand, and the verifier (server) does not need to use a dedicated authentication method. However, the configuration signals from external input will leak information to attackers, and also have the risk of being tampered with. In contrast, in the proposed design, configuration signals which are internally controlled cannot be obtained and manipulated from outside. From the mathematical model discussed in the previous section, when calculating the DCH PUF response, the delay vector and the real-time configurations (i.e., the real-time state of the LFSR) are required. According to general assumptions, an attacker knows the mathematical model of the PUF and the structure of the LFSR, and can collect CRPs without limitation. However, the attacker still does not know the real-time state of the LFSR, as the LFSR cannot be measured directly. In the first modeling experiment, we assume that the attacker already knows the real-time configurations. The modeling attack results using CMA-ES are shown in Figure 8. Later, we will show the cost of obtaining the real-time configurations.

#### TABLE 2. Hardware consumption (number of slices used on FPGA).  

<table>
<thead>
<tr>
<th>Structures</th>
<th>$N_{slice}$ with $n=1$</th>
<th>$N_{slice}$ with $n=2$</th>
<th>$N_{slice}$ with $n=3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Underlying n-XOR</td>
<td>129</td>
<td>259</td>
<td>388</td>
</tr>
<tr>
<td>APUF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5-bit DCH</td>
<td>137</td>
<td>268</td>
<td>400</td>
</tr>
<tr>
<td>6-bit DCH</td>
<td>137</td>
<td>268</td>
<td>400</td>
</tr>
<tr>
<td>7-bit DCH</td>
<td>141</td>
<td>272</td>
<td>400</td>
</tr>
<tr>
<td>8-bit DCH</td>
<td>141</td>
<td>272</td>
<td>400</td>
</tr>
<tr>
<td>9-bit DCH</td>
<td>142</td>
<td>273</td>
<td>401</td>
</tr>
<tr>
<td>10-bit DCH</td>
<td>150</td>
<td>273</td>
<td>407</td>
</tr>
<tr>
<td>11-bit DCH</td>
<td>150</td>
<td>273</td>
<td>407</td>
</tr>
</tbody>
</table>

#### FIGURE 8. CMA-ES modeling results of DCH PUFs with real-time configurations.

In Figure 8, each point represents the average prediction rate over 20 runs, where the 0-bit configuration refers to the conventional APUF design. For this design, it can be seen that when the real-time configurations are known, only a small amount of CRPs are needed to model the DCH structure efficiently. Even for the 15-bit DCH PUF structure, only 2,400 CRPs are needed to achieve a modeling accuracy of about 95 percent. In addition, in this experiment, the modeling time of each DCH PUF structure (based on APUF) is less than one minute.

In an on-board implementation, the LFSR may be in any state. This means that the real-time configurations of the DCH PUF are unknown. Hence, the attacker needs to preprocess the collected CRPs to obtain the real-time configurations. Here we provide two pre-processing methods, namely circular matching and CRP regrouping. For the DCH PUF structure with $n$-bit LFSR, assume that the LFSR can provide a maximum length sequence.

1) Circular matching. The collected CRPs are placed in order. The $2^n - 1$ sequential states (configuration signals) of the LFSR are calculated according to the feedback function. Next, circular matching is performed on the CRP set to obtain $2^n - 1$ sets of CRPs and configurations. These sets are used as the training data and input into the ML algorithm in turn, until the prediction rate is higher than 90 percent. The modeling results are shown in Table 3.

The time cost $T_{match}$ of modeling the dynamically configurable structure consists of two parts

$$T_{match} = T_{DCH} + \frac{2^n - 1}{2} T'_{DCH},$$

(18)

where $T_{DCH}$ is the time cost of training with correct configurations, and $T'_{DCH}$ is the time cost of training with incorrect configurations, which requires about 2,000 iterations. Since the required matching times are uniformly distributed from $1 \sim 2^n - 1$, the matching times are directly taken as half of the number of configurations $2^n - 1$, and then multiplied it by $T'_{DCH}$. It can be seen that the number of CRPs needed to
model the DCH PUF is only slightly more than that needed to model an XOR APUF of the same scale. But the time cost (calculation cost) is much higher than for the XOR APUF.

2) CRP Regroup. The CRPs collected are numbered from 1 to $2^n - 1$ in sequence. And put the CRPs with same sequence number together to form $2^n - 1$ new CRP sets, which are used for training respectively. For the simplest configuration (i.e., the traditional XOR APUF structure), there must be one set corresponding to it. CMA-ES is used for training, and the results are also shown in Table 3.

The time cost $T_{\text{regroup}}$ is obtained in two parts

$$T_{\text{regroup}} = T_{\text{XOR}} + \frac{2^n - 1}{2} T'_{\text{XOR}},$$

where $T_{\text{XOR}}$ is the time cost of modeling the traditional XOR APUF with a correct CRP set, and $T'_{\text{XOR}}$ is the time cost of modeling with an incorrect CRP set. Since the time needed to select the correct set is uniformly distributed in the range of $1 \sim 2^n - 1$, we directly take half of the number of sets $2^n - 1$, and then multiply by $T_{\text{XOR}}$. It can be seen that, compared with the circular matching method, the regrouping method saves a certain amount of time, but the number of CRPs needed is very large. With an increase of $n$ bits, the number of CRPs needed and the training time double.

From these two experiments, it can be seen that the designed DCH PUF structures have a good resistance to the CMA-ES ML modeling attack. Also, due to the particularity of the proposed design of the DCH structure, it cannot be attacked by other techniques typically applied against conventional PUF designs, as described next.

**Resistance to DNN Attack.** As a black box algorithm, DNNs do not need to know the mathematical model of a PUF. Simply by inputting a certain number of CRPs, a DNN attack can effectively simulate the relationship between the challenges and responses of a PUF, and predict its response accurately [20]. This is based on the premise that the relationship between the challenges and responses of the PUF structure is fixed (static). In our proposed dynamic design, after generating a one bit response, a new configuration will be generated to form a new PUF structure. In other words, all adjacent responses are generated by different PUF structures. Even if one challenge is input multiple times, the same DCH structure will generate different responses. Therefore, DNNs cannot model the DCH structure.

**Resistance to LR Attack.** Rührmair et al. [21] implemented an effective modeling attack against APUs and XOR APUs using LR, which is based on a special form of the APUF and XOR APUF’s output delay calculation. The DCH structure cannot be modeled using this approach, as discussed next. We will first analyze how LR works when attacking APUF and XOR APUF.

First of all, in APUF, the total difference in the delays (referred to as the decision delay) determined by the arbiter is shown in Eq. (2). When LR is used for training, the attacker uses the predicted APUF delay vector to calculate the predicted decision delay, and then inputs a sigmoid function to get a delay difference with the target response, which can be used to modify the predicted delay vector. The search

### Table 3. CMA-ES modeling results of XOR APUs and DCH PUFs with pre-processing of the CRPs.

<table>
<thead>
<tr>
<th>PUF structure</th>
<th>Pre-process</th>
<th>Number of CRPs</th>
<th>Prediction rate</th>
<th>Time cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>APUF</td>
<td>NA</td>
<td>800</td>
<td>94.35%</td>
<td>8 sec</td>
</tr>
<tr>
<td>2-XOR APUF</td>
<td>NA</td>
<td>$3 \times 10^3$</td>
<td>94.73%</td>
<td>30 sec</td>
</tr>
<tr>
<td>2-XOR lightweight secure</td>
<td>NA</td>
<td>$5 \times 10^3$</td>
<td>95.27%</td>
<td>2.6 min</td>
</tr>
<tr>
<td>3-XOR APUF</td>
<td>NA</td>
<td>$8 \times 10^4$</td>
<td>94.30%</td>
<td>9.9 min</td>
</tr>
<tr>
<td>3-XOR lightweight secure</td>
<td>NA</td>
<td>$8 \times 10^4$</td>
<td>98.45%*</td>
<td>2.3 hrs</td>
</tr>
<tr>
<td>4-XOR APUF</td>
<td>NA</td>
<td>$6 \times 10^4$</td>
<td>96.43%*</td>
<td>1.9 hrs</td>
</tr>
</tbody>
</table>

$^*$ CMA-ES running with 9,000 iterations. (Default with 5,000 iterations.)
space in this method is much smaller than that for CMA-ES, which is also the reason why LR can attack APUF and XOR APUF very efficiently.

In the $n$-stage $n$-XOR APUF, the responses of individual APUFs need to be determined first, and then XORed to obtain the final response. The LR algorithm cannot be used to model this APUF variant. However, the model of XOR APUF can be transformed, as follows:

$$R_{\text{xor}} = \begin{cases} 0, & \Delta_{\text{xor}}(m) > 0 \\ 1, & \Delta_{\text{xor}}(m) \leq 0 \end{cases} \quad (20)$$

$$\Delta_{\text{xor}}(m) = \prod_{i=1}^{n} \Delta_{\text{apuf}}(m). \quad (21)$$

Instead of XORing the multiple responses after the arbiters make their decisions, the delay differences of the individual APUFs can be multiplied, using the product as the decision delay of the XOR APUF. The final output can be determined by this decision delay (in the previous section, the self-XOR mathematical model we provided also uses this calculation method). Similar as the approach taken for APUF, during the training phase, the total decision delay is input into a sigmoid function to get the deviation between the current prediction delay vector and the target delay vector, and using this deviation the prediction model can be modified effectively.

This LR-based algorithm is efficient, but the format of its fitness function limits its application. In the proposed DCH structure, many configurations contain two overlapping FF loops. For such a structure, the calculation of final response cannot be transformed in a similar way as that detailed above, and further in [8] and [31], it is also reported that LR can only model non-overlapping FF APUF structures with fewer than 2 FF loops. Therefore, the LR-based ML algorithm in [21] cannot be used to model the DCH structure.

Resistance to Reliability-Based CMA-ES Attack. The reliability-based CMA-ES is an attack method proposed by Becker [24], which uses reliability information from the PUF structure instead of CRPs. In multi-XOR APUF structures, if a classical ML algorithm based on challenge response pairs is used for modeling, the number of CRPs needed will increase exponentially with an increase in the number of XORs. Therefore, when $n$ is large, such as $n > 10$, the XOR APUF is considered to be sufficiently resistant [18]. However, when using reliability-based CMA-ES to model the XOR APUF, the number of challenge-reliability pairs needed only increases linearly.

In this attack, each challenge is used repeatedly $m$ times, and the proportion of different responses in the statistical results is obtained. The challenge-reliability pairs reflect the switching possibility of the PUF response when different challenges are applied.

1) In APUF, it can be further inferred that the larger the switching probability, the closer the final decision delay is to 0. Therefore, when unstable challenges are used, the final decision delay can be constrained to different ranges around 0 according to the different switching probabilities.

2) In $n$-XOR APUFs, if the final response has flipped, it implies that at least one individual APUF response has flipped. Therefore, in the unstable challenge set collected, each challenge is responsible for at least one individual APUF’s flip. In other words, some challenges in this set will cause the same individual APUF to flip. In the training process, only one APUF delay vector is generated randomly, and its decision delay is limited to 0. After enough iterations, the vector may converge to one of the individual APUFs. By using the same challenge-reliability pairs set and running this algorithm multiple times, the delay vectors of multiple individual PUFs of the XOR APUF can be obtained.

Next, following the same approach, we will analyze if the reliability-based CMA-ES can be applied to the DCH structure. First, if a response bit is flipped in the APUF-based DCH structure, there are two reasons that can cause the switching: 1) the response of the main path including the FF loops is flipped; 2) the response of the SX branch is flipped. This shows that there are two kinds of unstable challenges in the set of challenge-reliability pairs, one is to make the decision delay of the main path approach 0, and the other is to make the decision delay of the SX branch approach 0. According to the steps, one of the two delay vectors is needed for training. However, unlike the decision delay calculation of APUF and XOR APUF, in the DCH structure, the decision delay calculation of the main path and SX branches must know the exact configuration information. This means that if an attacker tries to model the DCH PUF structure by using the reliability-based CMA-ES algorithm, they must first know the configuration of each challenge-reliability pair. However, the configuration information of the DCH structure cannot be obtained directly by an attacker. Therefore, we claim that the proposed DCH PUF structure is resistant to reliability-based CMA-ES modeling attacks.

V. DYNAMIC MATCHING AUTHENTICATION PROTOCOL

The various configurations in the proposed DCH PUF structure also bring challenges to its application in authentication protocols. In this section, we design an authentication protocol based on the dynamic DCH structure.

A. ENROLLMENT PHASE

In enrollment phase, the server first sends a sufficient number of challenges to the device side. The device sends the response and the corresponding configuration signal provided by the LFSR to the server. The server then trains the PUF model according to the response signal and the corresponding configuration, and stores the LFSR’s complete sequence. After the modeling is complete, the server/device communications link is removed. This enrollment process is shown in Figure 9. It should be noted that the signals from LFSR are not necessary for server to model the PUF, but with them, the modeling complexity is greatly reduced (refer to Section B).
B. AUTHENTICATION PHASE

During the authentication phase, as outlined in Figure 10, the server first sends a random nonce, $\text{Nonce}_b$, to the device. The device sends its ID $i$ and another random nonce, $\text{Nonce}_a$, to the server. The device side concatenates the two nonces and uses $\text{Nonce}_a \cdot \text{Nonce}_b$ as the challenge. According to the agreed response bit-length $N_{R0}$, the device side generates consecutive $N_{R0}$ bit responses $R_0$ from the PUF. Next, $R_0$ is placed at a random location in $R_a$, determined by a random index $\text{ind}_2$, with the remainder of $R_a$ padded with random numbers. $R_a$ is then sent to the server.

The server first verifies whether the ID of the device is in its stored list. Then, using $\{\text{Nonce}_a \parallel \text{Nonce}_b\}$ as the challenge, it calculates the response under all LFSR states according to the PUF model, and generates consecutive $R_b$ values. After receiving $R_a$, $N_{R0}$-bit substrings are matched with $R_b$ to get the maximum matching degree $T$. If $T$ is greater than the matching threshold $T_{th}$ set by the system, the authentication of the server to the device passes; otherwise, it fails. Next, the location index $\text{ind}^*_2 = \max\{\text{match}_{N_{R0}}(R_a, R_b)\}$ of the real response in $R_a$ is calculated and sent to the device, here $\text{match}_{N_{R0}}(R_a, R_b)$ means calculating the matching degrees between all $N_{R0}$ substrings in $R_a$ and $R_b$.

After receiving $\text{ind}^*_2$, if $|\text{ind}_2 - \text{ind}^*_2| > N_{th}$, the authentication of the device to the server passes, otherwise it fails.

Note that the authentication string, $R_a$, provided by the device includes the substring $R_0$ from the real response and padding with random bits generated by a TRNG, as shown in Figure 11. The starting position of the substring $R_0$ is determined by the number of clock cycles $\text{ind}_1$ and the previous status $S_{last}$ of the LFSR. After each generation of $R_a$, the device inputs a random number of $\text{ind}_1$ clock cycles to the LFSR to ensure that the next generated substring is random in the full response string $R_{full}$.

The proposed protocol differs from the Slender protocol [28], which also is a pattern matching based protocol:

- The proposed protocol uses the DCH PUF structure as the underlying PUF, and the random substrings of the responses are therefore generated from random configurations of the PUF. However, the Slender protocol uses a static PUF structure, and hence, its random substrings are generated from only one PUF structure.
- The proposed protocol generates $\text{ind}_1$ by inputting a random number of clock signals to its LFSR. The Slender protocol uses a TRNG to generate the random index $\text{ind}_1$.

VI. SECURITY ANALYSIS OF THE PROTOCOL

Recommended parameters for the proposed protocol are shown in Table 4. Based on these parameters, we will analyze the security of the protocol in this section. It is worth noting that since the underlying PUF structure we used is different from Slender protocol [28], the BERs of the implemented structures are not the same level. This means that the error tolerance required by the agreement is different. Therefore, the parameters proposed in this paper are quite different from Slender protocol.

A. ML ATTACK RESISTANCE

Classical ML Attack. To perform ML-based modeling of the proposed DCH PUF, multiple groups of delay vectors are randomly generated for one iteration of the protocol and the
group closest to the target delay vector is retained. To calculate which is closest to the target, challenges from the collected CRP set are substituted into the mathematical model of the PUF, and the most consistent response set is calculated. The fitness function, $f$ is

$$f = \sum_{i=1}^{n} \min(HD_{N_{R0}}(R_k, R_0)),$$

where $R_k$ is the complete response calculated according to the training model. The fitness function calculates the Hamming distance between all $N_{R0}$-bit substrings in $R_k$ and $R_0$. This calculation needs CRPs from the PUF structure, that is, the real response substring, $R_0$, from the authentication output in the protocol. However, as the proposed protocol uses random substrings, random positions and string padding, an attacker cannot know which part of the authentication bits string is the real response. If a sufficient number of correct responses are obtained by guessing, the number of possible combinations is

$$N_{comb} = \left( N_{Ra}(N_{Ra} - N_{R0}) \right)^{N_{min}/2}.$$

(23)

If the underlying structure is a 2-XOR APUF, and $N_{R0} = 64$ is selected, according to Table 3, the number of CRPs needed for modeling is 9,000, and $N_{comb} = (512 \times (512 - 64))^{9/2} = 229,376^{125}$. Such a large number makes it practically impossible to guess the correct configuration using exhaustive searching.

**New ML Attack Against Pattern Matching.** In [29], Becker proposed a new fitness function of the CMA-ES algorithm, where the Hamming weight of the authentication bits string is used instead of the direct response to reflect the accuracy of the prediction model. The new fitness function is

$$f' = corr(HW(R_k), HW(R_{th})).$$

(24)

where $HW(R_{th})$ represents a vector composed of Hamming weights of all elements of the vector $R_{th}$, and

$$HW(R_{th}) = \{HW(R_{th1}), HW(R_{th2}), \ldots \},$$

and equivalently for $HW(R_k)$. Since the Hamming weight calculation is independent of the random position of the set, the introduction of ind1 and ind2 cannot resist this modeling attack. With this method, the Slender protocol can be broken at a relatively lower cost [29].

We use the same fitness calculation from [29] to attack the protocol proposed in this paper. Table 5 shows the simulation results using MATLAB 2017b to perform the CMA-ES modeling. The inputs are blocks of authentication bits strings, where 1 block = 512 bits. The first four runs use the recommended parameters, and the last two runs use the parameters recommended in the Slender protocol. The experimental results show that Becker’s method [29] cannot break the proposed protocol. In the Slender protocol, different random substrings of the responses are generated by its only underlying PUF. Therefore, the HW vectors of the substrings and full responses have a certain correlation. However, in the proposed protocol, the different random substrings of the responses come from different PUF structures (that is the different configurations of the DCH PUF), and the HW vectors of the substrings are no longer related to each other, which makes this method valid.

### B. RANDOM GUESSING

The probability of successfully guessing the PUF response is related to the bit-length of the authentication bits string, the bit-length of the dynamic configuration values, the bit-length of the substrings, and the matching threshold. The probability that an attacker can determine the correct authentication response with random guessing is

$$P_{guess} = N_{Ra} \cdot (N_{Ra} - N_{R0}) \sum_{i=1}^{N_{R0}} \left( \frac{N_{Ra}}{2} \right) \left( \frac{1}{2} \right)^{N_{R0} - i}.$$

(26)

It will take an attacker $N_{Ra} \cdot (N_{Ra} - N_{R0})$ attempts to correctly guess the valid bit-string. Therefore, if the bit-length of the substring $N_{R0}$ is too small, the probability of a correct guess is increased. We have completed experiments for different $N_{R0}$ values when $N_{Ra} = 512$, and each authentication output is randomly guessed 10,000 times. The results are shown in Table 6. When $N_{R0}$ is less than or equal to 32, there will be a certain probability that the attacker will correctly guess all the valid bits, which will lead to a false acceptance. When $N_{R0}$ increases, the proportion of the number of bits guessed correctly by attackers decreases. When $N_{R0} = N_{Ra} = 512$, at most 317 bits are guessed correctly, accounting for only 61.91 percent.

### TABLE 4. Recommended protocol parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Symbol</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit-length of dynamic configurations</td>
<td>$N_{LSR}$</td>
<td>9</td>
</tr>
<tr>
<td>Bit-length of substring</td>
<td>$N_{R0}$</td>
<td>$64 \sim 512$</td>
</tr>
<tr>
<td>Bit-length of authentication bits</td>
<td>$N_{Ra}$</td>
<td>512</td>
</tr>
<tr>
<td>Matching threshold</td>
<td>$T_{th}$</td>
<td>$0.95 \sim 0.8$</td>
</tr>
<tr>
<td>Position error threshold</td>
<td>$N_{th}$</td>
<td>5</td>
</tr>
</tbody>
</table>

### TABLE 5. CMA-ES modeling results of proposed protocol when HW is used as fitness function.

<table>
<thead>
<tr>
<th>$N_{R0}$</th>
<th>$N_{R0}$</th>
<th>Inputs</th>
<th>Iterations</th>
<th>Prediction Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>512</td>
<td>64</td>
<td>$10^4$</td>
<td>5,000</td>
<td>52.38%</td>
</tr>
<tr>
<td>512</td>
<td>64</td>
<td>$2 \times 10^4$</td>
<td>9,000</td>
<td>51.06%</td>
</tr>
<tr>
<td>512</td>
<td>256</td>
<td>$10^4$</td>
<td>5,000</td>
<td>51.55%</td>
</tr>
<tr>
<td>512</td>
<td>256</td>
<td>$4 \times 10^4$</td>
<td>9,000</td>
<td>50.65%</td>
</tr>
<tr>
<td>1,250</td>
<td>10^4</td>
<td>5,000</td>
<td>51.73%</td>
<td></td>
</tr>
<tr>
<td>1,250</td>
<td>4 $\times 10^4$</td>
<td>9,000</td>
<td>51.73%</td>
<td></td>
</tr>
</tbody>
</table>
TABLE 6. Random guess authentication bits string matching results.

<table>
<thead>
<tr>
<th>$N_{00}$</th>
<th>Maximum Matching Bit Number</th>
<th>Error Tolerance</th>
<th>False Acceptance</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>16</td>
<td>-</td>
<td>99.99%</td>
</tr>
<tr>
<td>32</td>
<td>32</td>
<td>-</td>
<td>0.02%</td>
</tr>
<tr>
<td>48</td>
<td>43</td>
<td>10.42%</td>
<td>0</td>
</tr>
<tr>
<td>64</td>
<td>54</td>
<td>15.62%</td>
<td>0</td>
</tr>
<tr>
<td>128</td>
<td>96</td>
<td>25.00%</td>
<td>0</td>
</tr>
<tr>
<td>192</td>
<td>135</td>
<td>29.69%</td>
<td>0</td>
</tr>
<tr>
<td>256</td>
<td>174</td>
<td>32.03%</td>
<td>0</td>
</tr>
<tr>
<td>320</td>
<td>205</td>
<td>35.00%</td>
<td>0</td>
</tr>
<tr>
<td>384</td>
<td>243</td>
<td>36.72%</td>
<td>0</td>
</tr>
<tr>
<td>448</td>
<td>281</td>
<td>37.28%</td>
<td>0</td>
</tr>
<tr>
<td>512</td>
<td>317</td>
<td>38.09%</td>
<td>0</td>
</tr>
</tbody>
</table>

C. ERROR TOLERANCE

Another advantage of the proposed pattern matching based protocol is its high error tolerance. In other words, the accuracy of its authentication does not depend on error correction. By adjusting the threshold value for the degree of matching, an honest device can be identified at a certain bit error rate. The error tolerance of the proposed protocol is also shown in Table 6. For authentication bits strings of $N_{00} = 64$, the maximum matching over 10,000 random guesses is 54 bits, which means that when there are 10 unstable bits in the real response substring, $R_0$ of an honest device, by setting the matching threshold to $T_{th} = \frac{54}{64} = 84.38\%$, the honest device can still be identified while an incorrect acceptance of a dishonest device can be avoided. Also, as the bit-length $R_0$ increases, the error tolerance of the protocol improves.

VII. DISCUSSION AND CONCLUSION

Discussion. The dynamically configurable PUF design presented in this paper can be utilised with existing structures, such as the XOR APUF (shown in Figure 5) and the recently proposed interpose PUF [18] to improve security. It can also be used with the CRO PUF [32] and RRO PUF [11]. In a DCH PUF, the dynamic configuration signal is obtained by a LFSR and, although an attacker can derive the feedback function by analyzing the structure of the LFSR, the real-time configuration for each CRP remains unknown. This new dynamic authentication mechanism provides strong resistance to modeling attacks.

The proposed pattern matching based protocol has the following advantages: good error tolerance, no disclosure of the complete responses, and further increased resistance to ML attacks by the random selection of substrings and random padding. However, there are also potential disadvantages: for the same challenge, there are many combinations (any sufficient substring length of the complete response) that can be authenticated. This reduces the accuracy requirements of cloned PUF devices to a certain extent, and should be handled appropriately when designing protocols.

In the ML-based attacks mentioned above, CMA-ES is the most flexible one. It can be said that any strong PUF structure with a mathematical model will be threatened by CMA-ES. Its traditional approach is based on the information provided by CRPs, and that the fitness function of the CMA-ES algorithm is very flexible, which enables the derivation of more effective versions. For example, [24] proposed the use of a reliability-based CMA-ES algorithm, which is much more efficient than the traditional ML algorithms when attacking n-XOR APUFs with a large n. Moreover in [29], the new variant of CMA-ES with HW-based fitness function was capable of breaking the Slender protocol.

Conclusion. Almost all existing strong PUF structures have a static response behaviour. The proposed DCH structure achieves a dynamic PUF using a LFSR. The dynamic design does not conflict with existing structures, rather it can further improve their security. We also design a corresponding authentication protocol for the proposed dynamic PUF structure. The protocol based on matching pattern not only has strong resistance to traditional ML algorithms, but also resists the new variant of the CMA-ES algorithm. Overall, we demonstrate that the dynamic response mechanism and pattern matching can greatly increase the security of strong PUFs in authentication applications.

Reconfiguration is an effective mechanism to improve security for strong PUF structures, and can be achieved in various methods. However, it is challenging to realize the device identification and authentication without leaving enough information for attackers. At present, PUF design is facing high reliability requirements, and error correction mechanisms often consume a lot of hardware resources. With this concern, it is preferable to use an error-tolerant authentication protocol than to design highly reliable structure with a high cost. Moreover, by setting appropriate thresholds, another concerned aging issue can also be addressed by applying error-tolerant authentication protocol. Considering the incompatibility between different PUF structures and different authentication protocols, the collaborative design between PUF structure and authentication protocol will be a meaningful research direction, and which is also our future research direction.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation China under Grants 62022041 and 61771239.

REFERENCES


YIJUN CUI received the BS and PhD degrees in information engineering from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2010 and 2019, respectively. From 2014 to 2015, he was a visiting PhD student with Data Security System Group, Centre of Secure Information Technologies, Queen’s University Belfast, U.K. His current research focuses on hardware security.

MAIRE O’NEILL (Senior Member, IEEE) is currently the director with the UK Research Institute in Secure Hardware and Embedded Systems. She is the chair of Information Security and the research director with Data Security Systems, Centre for Secure Information Technologies, Queen’s University Belfast. She also leads the EU H2020 Secure architectures for Future Emerging Cryptography project. From 2008 to 2014, she held an EPSRC Leadership Fellowship and from 2003 to 2008, she was a former holder of a Royal Academy of Engineering research fellowship. She was the recipient of numerous awards for her research work which include the 2014 Royal Academy of Engineering Silver Medal and the British Female Inventor of the Year 2007. She has authored two research books and has authored or coauthored more than 130 peer-reviewed conference and journal publications. Her research interests include hardware cryptographic architectures, lightweight cryptography, side channel analysis, physical unclonable functions, post-quantum cryptography, and quantum-dot cellular automata circuit design. She is an associate editor for the IEEE Transactions on Computers and the IEEE Transactions on Emerging Topics in Computing. She is a member of the Royal Irish Academy and a Fellow of the Irish Academy of Engineering. She is also the program co-chair of IEEE ARITH 2020, and also the technical program committee member for ARITH, DATE, ASAP, ISCAS, ASP-DAC, ISVLSI, GLSVLSI, SIPS, NANOARCH, AICAS and ICONIP. He is a member of ASCOM and VSA Technical Committee of IEEE Circuits and Systems Society.

WEIQIANG LIU (Senior Member, IEEE) received the BSc degree in information engineering from the Nanjing University of Aeronautics and Astronautics (NUAA), Nanjing, China and the PhD degree in electronic engineering from the Queen’s University Belfast (QUB), Belfast, U.K., in 2006 and 2012, respectively. In December 2013, he joined the College of Electronic and Information Engineering, NUAA, where he is currently a professor and the vice dean with the college. He has authored or coauthored one research book by Artech House and more than 100 leading journal and conference papers. His research interests include approximate computing, hardware security and VLSI design for digital signal processing, and cryptography. His paper was selected as the Highlight Paper of IEEE TCAS-I in the 2021 January Issue and the Feature Paper of IEEE TC in the 2017 December issue. He was the recipient of the prestigious Excellent Young Scholar Award by the National Natural Science Foundation of China in 2020. He is currently an associate editor for the IEEE Transactions on Circuits and System I: Regular Papers (Jan. 2020–Dec. 2021), the IEEE Transactions on Emerging Topics in Computing (May 2019–Apr. 2021) and the IEEE Transactions on Computers (May 2015–Apr. 2019), a Steering Committee Member of IEEE Transactions on VLSI Systems (Jan. 2021–Dec. 2022). He is also the program co-chair of IEEE ARITH 2020, and also the technical program committee member for ARITH, DATE, ASAP, ISCAS, ASP-DAC, ISVLSI, GLSVLSI, SIPS, NANOARCH, AICAS and ICONIP. He is a member of ASCOM and VSA Technical Committee of IEEE Circuits and Systems Society.