electronics

MDPI

Article

Reliable and Modeling-Attack-Resistant Feed-Forward Crossbar Matrix Arbiter PUF for Anti-Counterfeiting Authentication

Xiang Yan, Cheng Zhang, Henghu Wu and Yin Zhang *

Hubei Collaborative Innovation Center for High-Efficiency Utilization of Solar Energy, Hubei University of Technology, Wuhan 430068, China; 102310256@hbut.edu.cn (X.Y.); 102410246@hbut.edu.cn (C.Z.); 102410244@hbut.edu.cn (H.W.)

* Correspondence: zhangyin@hbut.edu.cn

Abstract

Physical Unclonable Functions (PUFs) represent a highly promising hardware security primitive, yet they face constraints of insufficient reliability and threats from modeling attacks. This paper designs a novel Feed-Forward Crossbar Matrix Arbiter PUF (FC-MA PUF). It incorporates an inter-stage crossbar structure, a feed-forward control system, and a mechanism for selecting reliable challenge-response pairs. These features significantly enhance the structural non-linearity and stability, substantially improving security and adaptability to a wider range of operating environments. It provides a high-strength authentication solution with low resource overhead for lightweight security-demanding devices such as IoT devices. The proposed FC-MA PUF has been successfully implemented on a Field-Programmable Gate Array (FPGA) platform. Experimental results for the selected 4-stage FC-MA PUF configuration show a bias, inter-chip uniqueness, and bit error rate (BER) of 49.88%, 49.68%, and 0.018%, respectively. Furthermore, the structure allows for flexible configuration of the number of feed-forward modules based on practical application requirements: a greater number of feed-forward modules enhances security but also leads to an increased BER and a decreased proportion of stable challenge-response pairs. Experimental results based on a training set of 1,000,000 challenge-response pairs demonstrate that: with two feed-forward units, the stable (Challenge Response Pair)CRP ratio is 39.72% and the Covariance Matrix Adaptation Evolutionary Strategies (CMA-ES) attack prediction success rate is 58.20%; with three units, the ratio decreases to 29.12% and the prediction rate drops to 54.91%; with four units, these values further decline to 20.18% and 52.33% respectively. These results confirm that the proposed FC-MA PUF effectively resists multiple modeling attacks, including Logistic Regression (LR), Support Vector Machine (SVM), and CMA-ES.

Keywords: physically unclonable functions; modeling-attack-resistant; reliability enhancement

Check for updates

Academic Editor: Paris Kitsos

Received: 15 February 2026
Revised: 16 March 2026
Accepted: 17 March 2026
Published: 26 March 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

The Physically Unclonable Function is an important hardware security primitive that generates unique and unclonable identifiers for electronic devices by exploiting inherent manufacturing process variations. It is widely employed in applications such as anti-counterfeiting authentication, cryptographic key generation and storage, and intellectual property protection [1]. Based on the capacity of Challenge-Response Pairs, PUFs can be categorized into weak PUFs and strong PUFs. Strong PUFs, capable of supporting a vast number of CRPs, are particularly suitable for lightweight authentication and similar

scenarios. The most representative strong PUF architecture is the Arbiter PUF (APUF). However, conventional APUFs are vulnerable to machine learning (ML)-based modeling attacks, where an adversary can clone the PUF behavior by collecting a subset of CRPs [2], posing a serious threat to security. In addition to hardware-based primitives such as PUFs, lightweight security schemes based on nonlinear dynamical systems have also attracted attention in recent years. For instance, a four-dimensional Hénon memristor map [3,4] has been applied to lightweight image encryption, demonstrating that nonlinear structures can enhance security while maintaining low implementation cost.

To enhance resilience against modeling attacks, existing PUF's research primarily follows two directions: first, structural enhancement, such as increasing decision complexity through parallel multi-path structures with nonlinear operations (e.g., XOR-APUF [5]) or dynamic path selection (e.g., Multipath PUF [6]); second, challenge obfuscation, which processes the original challenge to control the PUF, for instance, by feeding the response of a preceding stage as the challenge to a subsequent stage (e.g., IPUF [7]) or dynamically reconstructing the challenge-response mapping [8]. Nevertheless, these approaches often introduce notable drawbacks alongside security improvements: MPUF-like structures incur substantial hardware overhead, making them difficult to deploy in resource-constrained devices [9]; while challenge-obfuscation designs frequently suffer from insufficient stability and high bit-error rates (BER), necessitating error-correction techniques such as Bose–Chaudhuri–Hocquenghem (BCH) codes [10] or fuzzy extractors [11], which add extra cost and may impact practicality.

Recently, the Crossbar Matrix Arbiter PUF (CMAPUF) has been proposed to achieve higher complexity and stability with limited resources, employing inter-stage crossbar connections and an externally provided path-selection signal to dynamically switch transmission paths [12]. However, in this architecture, the path-selection signal is exposed at the external interface. If obtained by an attacker, it could undermine the randomness of path selection, thereby reducing the practical effectiveness against modeling attacks. On the other hand, internal feed-forward (FF) control offers a lightweight approach to enhance nonlinearity and security [13]. Yet traditional feed-forward PUFs are prone to systematic bit errors due to arbiter metastability [14–16], often requiring a limitation on the number of FF units or the introduction of error-correction mechanisms, which constrains reliability gains and resource efficiency.

To simultaneously achieve high security, high reliability, and low hardware overhead, this paper proposes a novel Feed-Forward Crossbar Matrix Arbiter PUF. The design integrates a crossbar matrix path structure with an internal feed-forward control mechanism. It dynamically enhances the combinatorial complexity of transmission paths while employing an improved FF module to generate implicit path-control signals in real time, equipped with metastability detection capability. As a result, the proposed structure significantly reduces systematic bit errors while boosting nonlinearity and resistance against modeling attacks. A systematic theoretical analysis and mathematical modeling of the FC-MA PUF are presented to elucidate its security mechanisms and performance advantages. The circuit is successfully implemented and tested on an Xilinx Artix-7 FPGA. Experimental results demonstrate that the proposed structure exhibits high uniqueness, uniformity, and reliability compared to existing PUFs with cross-feedback loops, while incurring only minimal additional hardware overhead. Due to its lightweight hardware cost and strong device-unique characteristics, the proposed FC-MA PUF is also suitable for securing resource-constrained edge devices in distributed energy systems, such as photovoltaic inverter controllers, smart meters, and data acquisition nodes in solar power networks. In such scenarios, the PUF can provide hardware-rooted device authentication to prevent node spoofing and unauthorized device replacement.

The subsequent sections of this paper are organized as follows: Section 2 reviews the principles of the APUF and its variants; Section 3 elaborates on the proposed novel structure and its operational mechanism; Section 4 presents the implementation method, experimental results, analysis, and provides a conclusion.

2. Background

2.1. Arbiter PUF

The Arbiter PUF [17] is a core representative of strong PUFs. Its unique responses rely entirely on the irreproducible process variations inherent in integrated circuit manufacturing. As shown in Figure 1, this structure consists of *N*-stage of symmetrical switches. Each stage contains two multiplexers and one control bit Challenge, which determines whether the signals pass through straight or are cross-transmitted. Although the two paths are designed to be perfectly symmetrical, minor deviations during the actual manufacturing process introduce random delay differences. When the signals reach the end, the arbiter captures the subtle arrival time difference between the paths, converting the analog delay into a digital response output (0/1).

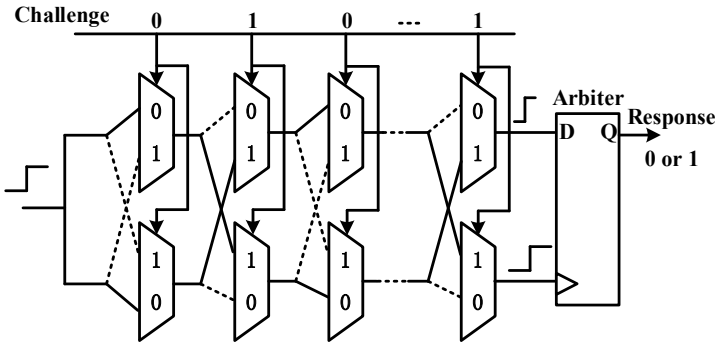


Figure 1. *N*-stage Arbiter PUF structure.

2.2. APUF with Complex Path Structure

To achieve higher security and complexity enhancement with relatively low resource overhead, the CMA PUF was proposed as a novel Arbiter PUF structure. As shown in Figure 2, it employs a path reconfiguration mechanism to increase its internal complexity, thereby effectively strengthening its overall protective capability. Its core innovation lies in constructing a dual-row, *N*-stage arbiter array to form four geometrically symmetrical delay paths and introducing an inter-stage inter-row interconnection network.

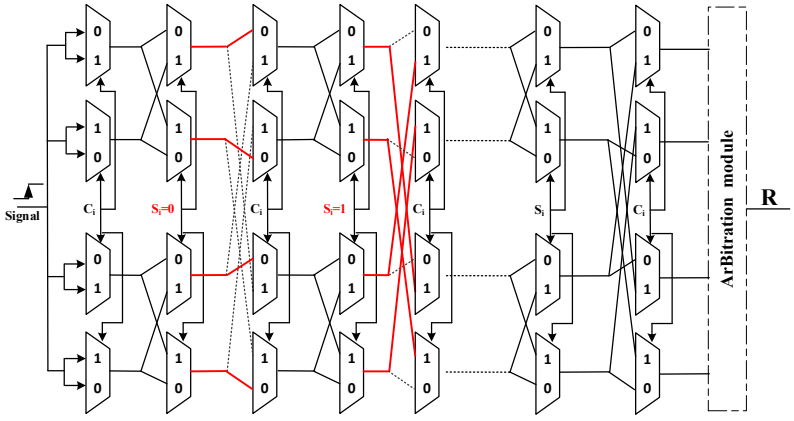


Figure 2. *N*-stage CMA PUF structure.

This design [12] utilizes an external selection signal "*S*" to dynamically control the transmission mode: when $S = 0$, signals transmit within their native row, maintaining the path constraints of a traditional Arbiter PUF; when $S = 1$, inter-row signal exchange is activated, allowing input signals to cross-transmit between the two rows. This reconfigurable topology expands the path combinations from two paths to four paths, generating an exponentially growing path bifurcation space. As the number of paths increases, the modeling complexity also rises accordingly, serving the purpose of resisting modeling attacks. However, the potential exposure risk of the path selection signal *S* undermines its efforts against modeling attacks.

2.3. Feed-Forward PUF

To counter increasingly advanced attack methods, incorporating feedback signals within the PUF structure to interfere with attackers is an effective strategy. A typical structure is the feed-forward PUF (FF-PUF), shown in Figure 3, which resists machine learning attacks by cascading feed-forward arbitration modules. It embeds these feed-forward arbitration modules between the stages of a traditional Arbiter PUF. These modules capture the arrival time difference in the competing paths in real-time, generating a 1-bit control signal that serves as a challenge input for subsequent stages. This design partially conceals the original challenge, forcing attackers to accurately model the path delays of preceding stages to predict the feed-forward signal, thereby creating a protective barrier. Its lightweight nature makes it well-suited for resource-constrained IoT devices, while delivering considerable effectiveness. However, the instability of the feed-forward signal can degrade the reliability of the PUF's output response.

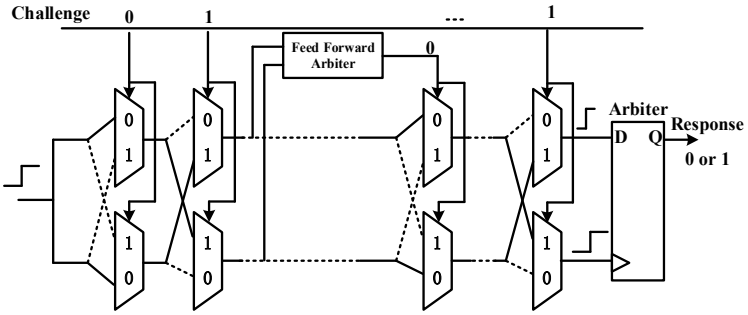


Figure 3. *N*-stage FF Arbiter PUF structure.

2.4. Machine Learning Attacks Against APUF-Type Structures

The mathematical model of the Arbiter PUF is inherently a linear superposition system. This linear separability makes it an ideal target for machine learning attacks: an attacker can efficiently model the weight vector w by collecting a subset of CRPs, achieving complete cloning of the PUF's behavior. The Logistic Regression attack proposed by Rührmair et al. [2] models the response decision boundary as a linear hyperplane $R = \mathrm{sgn}(w^{\mathrm{T}} \cdot \Phi(c))$. By minimizing the hinge loss function, only 2000 CRPs are required to break a 64-stage APUF within 0.6 s with an accuracy greater than 99%.

In recent years, deep learning-enhanced attacks have significantly improved the ability to counteract environmental noise interference, further exacerbating the security risks of traditional Arbiter PUFs. SVM) [18] is a powerful tool for solving classification problems; for attacks targeting APUFs, each response bit can be treated as a binary classification problem [10]. The Radial Basis Function (RBF) [19] kernel can map data into a high-dimensional space to address linear inseparability in the original feature space.

Deep Neural Networks (DNN) [20,21] are considered one of the most powerful black-box attack methods. They leverage multi-layer abstract neural networks to learn data

features and generate separating hyperplanes through binary classification models. As long as the PUF's data function is linearly separable, a DNN can successfully attack it. Therefore, the overall circuit structure must possess sufficient non-linearity and complexity to effectively resist attackers.

3. Research on Collaborative Architecture Design and Attack-Resistant Mechanisms

3.1. Feed-Forward Crossbar Matrix PUF Circuit with a Triple-Protection Mechanism

To simultaneously achieve high security, high reliability, and low hardware overhead, this paper proposes a novel FC-MA PUF. The architecture establishes a core protection chain against modeling attacks through three integrated defense mechanisms: (1) A metastability-aware feed-forward network that converts intrinsic process variations into real-time control signals, governing subsequent transmission paths to enhance structural non-linearity. (2) An inter-stage interleaved path topology that dynamically reconfigures transmission links, thereby breaking the traditional linear delay model. (3) A dynamic response-reliability selecting mechanism, which detects unstable response bits in real time and outputs a reliability flag. Downstream circuits can use this flag to extract only reliable responses. This approach not only reduces the bit-error rate but also mitigates the risk of successful attacks via intentional environmental perturbations such as voltage or temperature injection.

3.1.1. Overall Structure

The FC-MA PUF architecture proposed in this paper, as shown in Figure 4, employs a dual-row, *N*-stage Arbiter PUF to construct four symmetrical delay paths, and incorporates distributed multi-bit feed-forward arbitration modules at selected stages *i*. Each FeedForward (FF) module generates a 6-bit path control signal S based on the delay differences in the four pulse signals. This signal *S* directly controls the path switching switches in subsequent stages. These control signals function at key inter-stage points: when $S = 0$, signals transmit within their native row; when $S = 1$, inter-row exchange is activated. This mechanism breaks the traditional linear delay propagation mode of the APUF and significantly expands the path combination space, achieving path complexity and thereby enhancing the structure's resistance to modeling attacks.

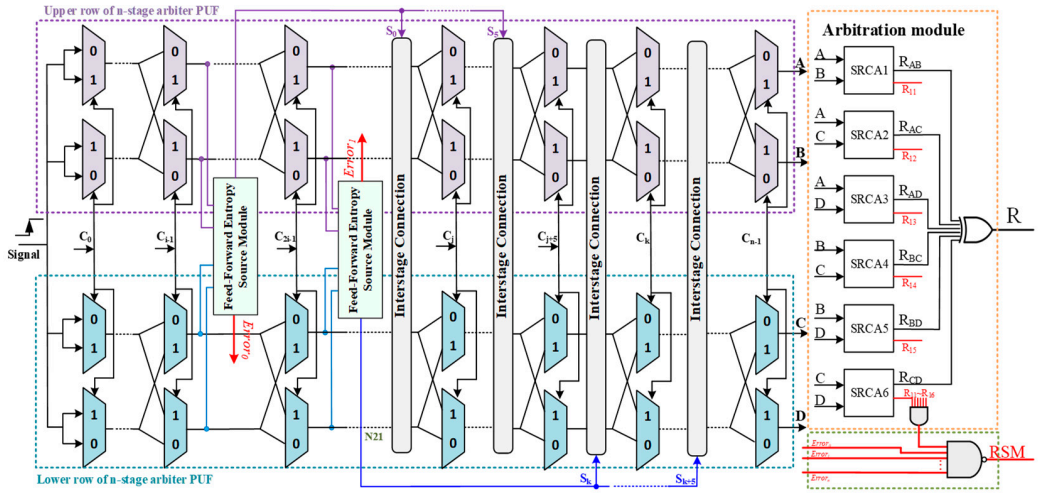


Figure 4. Overall FC-MA PUF circuit.

All arbitration units in this PUF's circuit structure employ metastability-aware SRCA modules. The metastability detection bits from each module are collected and processed to generate a global reliability indicator signal, RSM (Response Stability Metric), which

flags whether the current challenge-response pair is stable and reliable. To reduce the probability of generating unreliable CRPs, the value of stage interval i should not be too small, as excessively short total path delays before the arbitration module may result in minimal signal delay differences. This increases susceptibility to metastability-induced arbitration errors and consequent bit errors. Finally, the arbitration module utilizes a four-path differential XOR arbiter to perform pairwise arbitration on all possible combinations of the delay paths, with the arbitration results nonlinearly combined through XOR operations to produce the final response bit R.

Building upon the structural description above, we now clarify the role of each architectural component. The crossbar inter-stage structure primarily enhances path diversity by expanding the delay competition from two to four candidate paths, thereby increasing structural entropy and modeling complexity. The feed-forward control modules introduce dynamic path dependency, which amplifies inherent process variations into stage-dependent nonlinear perturbations, significantly reducing linear separability exploited by machine learning attacks. The SRCA-based arbitration units improve temporal stability by explicitly detecting metastable conditions, while the global RSM screening mechanism reduces the effective bit error rate by filtering unstable CRPs. The final XOR-based arbitration further increases decision boundary discontinuity. Through this collaborative design, the architecture achieves a balanced trade-off among modeling resistance, reliability, and hardware overhead.

3.1.2. Inter-Stage Connection Structure

This design increases information entropy by reconstructing the inter-stage delay path transmission structure, as shown in Figure 5a. When the inter-stage cross-transmission mode is not activated, the input signals follow the path constraints of the classical APUF—the upper and lower row delay paths are isolated from each other, and the challenge bit C_i only controls the intra-row transmission mode. When the inter-stage cross-transmission mode is activated, the control signal Si drives a symmetrical crossbar switch. The specific implementation method is shown in Figure 2, and its configuration rule is: the I0/I1 ports input path signals, and the I2 port inputs S_i. As shown in Figure 5b,c, the Boolean state of S_i (0/1) directly determines the signal transmission mode—S_i = 0 maintains inter-row isolation, while S_i = 1 activates inter-row signal exchange.

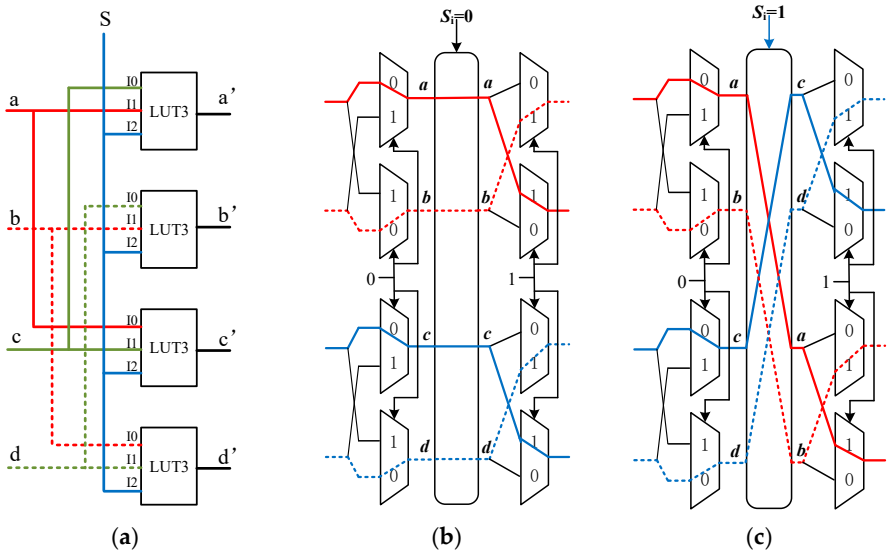


Figure 5. Reconfigurable Inter-Stage Structure (**a**) LUT3 Implementation Schematic (**b**) Signal Transmission Path for S = 0 (**c**) Signal Transmission Path for S = 1.

This dynamic path switching expands the delay competition from two paths to four paths, and its symmetrical crossbar topology helps ensure good output bias. The value of this architecture lies in two aspects: Firstly, the inter-stage connection structure adopts a symmetrical crossbar method, guaranteeing the generation of unbiased output. The structure supports signal transmission between the two APUF rows: the randomness and diversity introduced by inter-row signal transmission and cross-feed loops can significantly enhance entropy source diversity. Secondly, the construction of the four-path delay pool provides the hardware foundation for implementing single-stage, multi-bit feed-forward control.

3.1.3. Feed-Forward Entropy Source Module with Metastability Detection

This design aims to generate a multi-bit feed-forward control signal by constructing a four-path delay arbitration feed-forward network, thereby strengthening the architecture's defense against modeling attacks. As shown in Figure 6, this mechanism dynamically generates the control signal *S* by constructing a four-path delay sensing feed-forward network that captures the speed differences between all pairs of the four paths in real-time. This mechanism compares the delay differences in the four symmetrical delay paths to generate a 6-bit signal *S* used to control the inter-stage connection structure. This signal S is then output to the subsequent crossbar interconnection module. Based on the instantaneous speed difference, *S* dynamically switches the inter-row connections, causing the same challenge signal to produce different transmission paths on different PUF instances. The generation of signal *S* causes the process variations from preceding stages to be amplified into random perturbations that are difficult to model during the response arbitration process within the FF module. This method breaks the static mapping assumption relied upon by machine learning attacks, forcing the attack model to simultaneously fit complex path timing behaviors and distributed process entropy perturbations, thereby significantly increasing the modeling complexity.

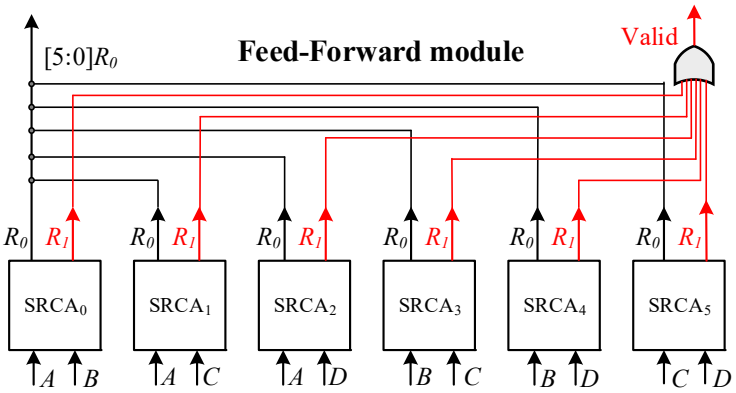


Figure 6. Feed-Forward Arbitration Module.

The output stability of the feed-forward entropy source directly affects the overall system bit error rate, making its stability a top priority. This study proposes replacing the traditional D Flip-Flop (DFF) arbiter with an SR Latch-based Composite Arbiter (SR-CA) structure. As shown in Figure 7, this structure forms an SR latch using cross-coupled NOR gates and cascades two DFFs to create a falling-edge-triggered detection mechanism. When the falling edge of the test pulse arrives, if the two competing signals S and R transition from high to low level nearly simultaneously, the SR latch enters a metastable state characterized by high-frequency oscillations. At this point, the dual DFFs act as a frequency counter to capture the oscillating signal: the first-level DFF outputs $R^0_{d,n} = 1$ due to the advantage in sampling the high-level duration within the oscillation period, and the second-level DFF,

after detecting the oscillatory characteristic from the Q output of the first DFF, outputs $R^1{}_{d,n}$, thereby encoding the metastability into the unique state "11".

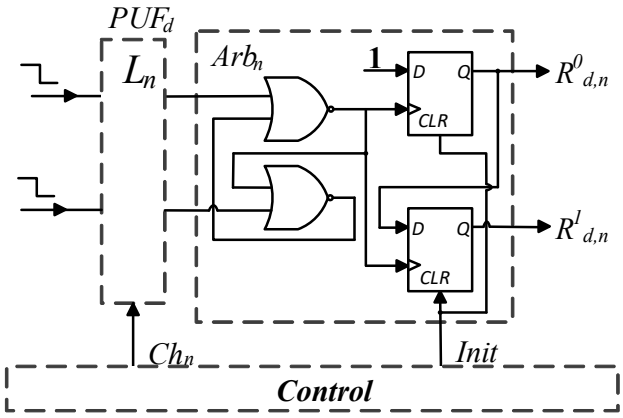


Figure 7. Structure of the SR Latch-based Composite Arbiter (SRCA).

Compared to the susceptibility of traditional DFF arbiters to metastability interference, this design enables metastability detection: when the delay difference between the upper and lower paths is significant, $R^0{}_{d,n}$ outputs a stable 1 or 0, and $R^1{}_{d,n}$ outputs 0. When the delay difference between the upper and lower paths is small, the SR latch oscillates. The dual DFFs act as frequency counters, where the first DFF triggers multiple times during the oscillation period. Because the D input of the second DFF is connected to the Q output of the first DFF, and Q is oscillating, this causes the output $R^1{}_{d,n}$ to be 1, indicating that this arbiter has entered a metastable state. This three-state encoding directly indicates the potential presence of risk within the system. The state "11" signifies that arbitration resulted in metastability, meaning the generated response signal is unreliable and susceptible to voltage and temperature (V&T) variations. All reliability indicator bits (from multiple such modules) are ultimately fed into a NOR operation to generate the final global reliability flag.

3.2. Mechanism Reliable CRPs Screening Mechanism

Within the FC-MA PUF architecture, the design of the global reliability indicator signal "RSM" aims to identify unstable CRPs and filter them out, retaining only highly stable CRPs to ensure the overall structural stability. The RSM signal is generated by performing a NOR logic operation on the diagnostic bit outputs from all SRCA modules. It serves to flag whether the current challenge-response pair is stable. During the production enrollment phase, the RSM signal is bound as key data to the raw CRP and reported to the authentication server. If RSM = 0, it indicates that the current CRP carries a potential risk of bit errors, and the system automatically discards this high-risk CRP. Only stable CRPs with RSM = 1 are retained for subsequent identity authentication processes.

Since the RSM signal is not exposed during the runtime authentication process, adversaries with black-box query access cannot observe this stability indicator, nor can they exploit noise-induced response variations to enhance modeling attacks. This design, by preemptively excluding unreliable responses, not only ensures the determinism of PUF outputs at the source and significantly reduces the system's bit error rate, but also strengthens the security foundation while maintaining high reliability: a stable CRP database directly undermines the feasibility of machine learning attacks, as the attack model cannot leverage behaviors such as noise-induced response flipping to accelerate model compromise.

3.3. Mathematical Analysis of the FC-MA PUF

To clarify the scope of our security claims, we explicitly define the threat model considered in this work. We assume a strong black-box adversary who:

1. Can adaptively query the PUF and collect a polynomial number of challenge–response pairs (CRPs).
2. Has full knowledge of the circuit architecture.
3. Can apply state-of-the-art machine learning algorithms (e.g., LR, SVM, DNN, CMA-ES).
4. Does not have physical access to internal delay measurements.
5. Cannot directly observe or manipulate the internally generated feed-forward control signals.

Under this threat model, the adversary's goal is to construct a predictive model achieving significantly better-than-random accuracy on unseen challenges. The security claims of this paper are restricted to resistance against modeling attacks under the above assumptions. No claim of cryptographic or information-theoretic provable security is made.

The preceding sections have detailed the system architecture. To evaluate the robustness of this architecture against adversarial machine learning attacks, this section conducts a formal verification based on a mathematical framework. The FC-MA PUF deconstructs the linear separability of the traditional Arbiter PUF (APUF) through a triple mechanism: configurable path topology, feed-forward entropy source control, and XOR-based nonlinear decision-making. The delay difference model of the traditional APUF is a linear system [22], where the path delay difference $\Delta\tau$ is a linear combination of the process variation weight vector w and the path feature vector:

$$\Delta\tau_{APUF} = w^T \cdot \Phi(c) + \Delta\tau_0 \tag{1}$$

Here, $\Delta\tau_0$ represents the inherent arbiter bias, and the path feature vector Φ(c) is statically mapped from the challenge bits c. The response output satisfies:

$$R = sgn(\Delta\tau) = sgn(w^T \cdot \Phi(c) + \Delta\tau_0) \tag{2}$$

This static path selection mechanism constrains the decision boundary to the hyperplane $w^T \cdot \Phi(c) + \Delta\tau_0 = 0$, enabling efficient modeling attacks via linear separability. To overcome this limitation, the FC-MA PUF introduces a dynamic path selection function:

$$\Phi_i = \Gamma(S_i) \cdot \Lambda(C_i) \tag{3}$$

The intra-row routing matrix $\Lambda(C_i)$ and the inter-stage crossbar matrix $\Gamma(S_i)$ are defined as:

$$\Lambda(C_i) = \begin{bmatrix} (1-c_i) & c_i & 0 & 0 \\ c_i & (1-c_i) & 0 & 0 \\ 0 & 0 & (1-c_i) & c_i \\ 0 & 0 & c_i & (1-c_i) \end{bmatrix} \tag{4}$$

$$\Gamma(S_i) = \begin{bmatrix} (1-S_i) & 0 & S_i & 0 \\ 0 & (1-S_i) & 0 & S_i \\ S_i & 0 & (1-S_i) & 0 \\ 0 & S_i & 0 & (1-S_i) \end{bmatrix} \tag{5}$$

This structure expands the single-stage signal transmission topology from traditional binary selection to a four-path combination, creating an exponentially growing path bifur-

cation space. The FF module generates a 6-bit entropy control signal vector by pairwise comparison of the cumulative propagation delay differences among the four delay paths:

$$S_i[k] = \left[sgn\left(\tau_{i-1}^{p_k} - \tau_{i-1}^{q_k} \right) \right] for\ k = 0\ to\ 5,\ (p_k, q_k) \in M \tag{6}$$

$$M = \{(A,B),(A,C),(A,D),(B,C),(B,D),(C,D)\}$$

Here, $\tau_{i-1} = \sum_1^{i-1} w_i \Phi_i$ represents the cumulative path delay from stage 1 to stage $i-1$ for path p, and (p_k, q_k) denotes an ordered pair of paths. For example, signal S_0 is generated by arbitrating the delay difference between paths A and B. This mechanism dynamically converts the random process variations wi introduced during manufacturing into entropy control signals via cascaded feedback. These signals control the inter-stage crossbar module to achieve dynamic switching of the four paths. The final response is obtained through XOR-based joint arbitration of the four paths:

$$R = F_{XXPUF}(\vec{c}) = \bigoplus_{k=1}^{6} sgn\left(\sum_{i=1}^{n} \omega_i \cdot \Phi_i(\vec{C_I}, \vec{S_I}) + \Delta\tau_0^{(k)} \right) \tag{7}$$

Here, $\Phi_i(\vec{C_I}, \vec{S_I})$ is the dynamic path function jointly controlled by the challenge bit C_i and the feed-forward signal S_i. ω_i is the equivalent weight of the process variation at stage i, and $\Delta\tau_0^{(k)}$ represents the inherent delay bias of the k-th arbiter.

This architecture significantly expands the path selection space via the dynamic path generation mechanism, forcing attackers to construct higher-dimensional parameter models for effective attacks. Furthermore, the feed-forward arbitration module captures perturbations from preceding process noise. The control signals generated by the inherent randomness of physical properties eliminate deterministic influences on subsequent path selection, producing unpredictable dynamic paths. This exponentially increases the prediction accuracy required by machine learning models for preceding stages, thereby enhancing the overall structure's resistance to modeling. All path outputs undergo XOR logic operations to generate the final response R. This nonlinear operation introduces high discontinuity into the decision boundary, making the structure difficult to partition linearly. Theoretical analysis demonstrates that the FC-MA PUF introduces dynamic path dependency, distributed nonlinearity, and XOR-based decision discontinuity, which jointly increase the hypothesis space required for successful modeling. While this does not constitute a formal cryptographic security proof, it provides a structural basis explaining the empirical resistance observed in Section 4.

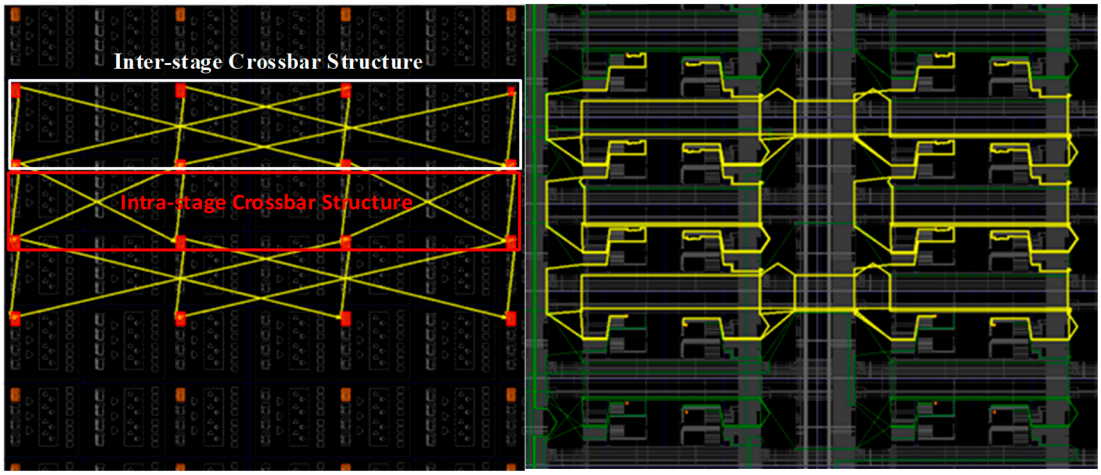
The above derivation provides an upper-bound estimation under the assumption of independent feed-forward control signals. In practice, since feed-forward signals are generated from preceding delay comparisons, certain statistical correlations may exist, potentially reducing the effective number of independent paths. Nevertheless, the exponential growth trend relative to classical APUF structures remains valid, and experimental modeling results confirm the substantial increase in structural nonlinearity.

4. Implementation and Experimental Results

This study implemented and evaluated the proposed PUF architecture on the Xilinx Artix-7 FPGA platform. PUF instances were developed using Verilog HDL in the Vivado design environment, with the core structure deployed in FPGA logic slices (SLICEs). Each crossbar stage was constructed by instantiating LUT3 primitives. A total of 100 independent 64-stage PUF instances were uniformly distributed across 10 FPGA development boards, with 10 instances per board. Systematic evaluations were conducted on core performance metrics, including uniformity, reliability, and uniqueness. Additionally, post-screening of

reliable CRPs enabled comprehensive testing of four key indicators: uniformity, reliability, uniqueness, and resistance to modeling attacks.

To optimize the performance-security balance, a configurable feed-forward control mechanism was introduced. By dynamically adjusting the number of feed-forward stages, this mechanism co-optimizes modeling-attack resistance and operational reliability. At the physical implementation level, customized Vivado scripts enforced placement constraints on LUT coordinates and input ports, focusing on delay matching for symmetrical paths to suppress systematic bias induced by asymmetric layout. Figure 8a visually contrasts the inter-row crossbar structure with a non-crossbar layout, while Figure 8b provides corresponding low-level interconnect visualizations.



(**a**) (**b**)

Figure 8. FC-MA PUF Placement and Routing Diagram: (**a**) Floorplan View. (**b**) Transistor-Level Interconnect Visualization.

4.1. Reliability

Reliability refers to the temporal repeatability or stability of responses to the same input challenge. It can be quantified using the Bit Error Rate (BER), defined as the average percentage of erroneous response bits obtained across different time intervals or operating environments:

$$BER = 1 - Reliability = \frac{1}{k}\sum_{j=1}^{k}\frac{HD\left(R, R'_j\right)}{n} \times 100\% \quad (8)$$

where R is the n-bit reference responses obtained in the reference condition. R'_j is the n-bit response obtained by varying the temperature or voltage, HD (R, R'_j) is the hamming distance (HD) between R and R'_j.

Reliability experiments were conducted under controlled voltage and temperature sweeps. The temperature range was varied from −15 °C to 90 °C with 15 °C steps, and the supply voltage was swept from 0.95 V to 1.05 V with 0.0125 V increments. At each operating point, a stabilization time of 5 min was allowed before measurement. Each challenge–response pair was then evaluated 100 times at each voltage and temperature point to compute the bit error rate according to Equation (8). Experiments were performed across 10 independent FPGA boards, and the reported BER values represent the average across boards. Unless otherwise specified, all BER results reported in figures and tables correspond to CRPs that satisfy the RSM screening condition (RSM = 1); unscreened CRPs were excluded from statistical evaluation.

To quantitatively evaluate the effect of FF modules on the overall reliability of the PUF, additional experiments were designed by varying the number of FF units under the same voltage and temperature conditions. A test dataset of 10,000 CRPs was employed, with each CRP measured 100 times to calculate the average bit error rate.

The results demonstrate that metastability screening requires progressively higher exclusion rates as FF units increase. This necessitates traversing a larger CRP pool during device enrollment to identify stable pairs, with stable CRP ratios measured at 39.72% for 2 FF units, 29.12% for 3 FF units, and 20.18% for 4 FF units, as illustrated in Figure 9. Environmental stability tests under varying conditions reveal that while BER increases exponentially with additional FF stages, the system maintains 0.018% BER at room temperature and nominal voltage with 4 FF units. This confirms that the reliability cost incurred to enhance modeling-attack resistance remains within acceptable operational limits.

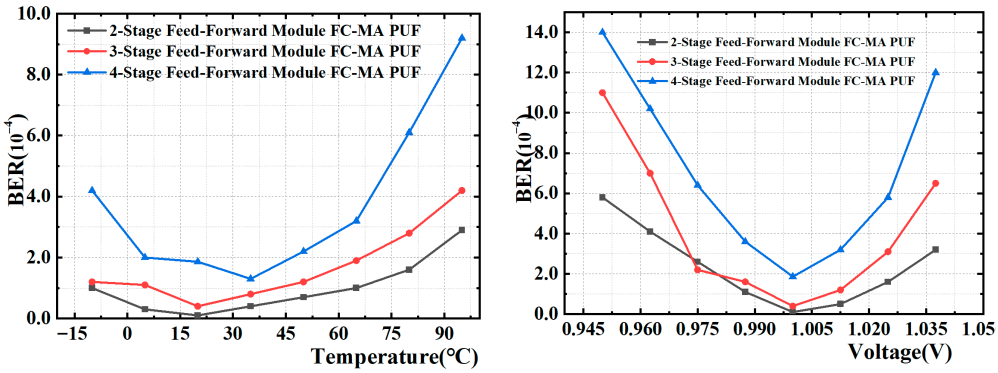


Figure 9. Reliability of PUF Structures with Varying Numbers of FF Units: (**a**) BER Across Temperature Variations; (**b**) BER Across Voltage Variations.

The FC-MA architecture, therefore, exhibits an inherent tradeoff among modeling resistance, reliability, and stable CRP availability. Increasing the feed-forward depth enhances structural nonlinearity and strengthens resistance to modeling attacks, but reduces the proportion of stable CRPs due to increased delay sensitivity. Nevertheless, since the original challenge space is 2^{64}, even a stable ratio of approximately 20% yields an absolute number of usable CRPs far exceeding practical authentication requirements.

In realistic deployments, only a limited subset of stable CRPs (e.g., on the order of 10^{-4}) is required per device. Therefore, CRP availability does not become a bottleneck under the evaluated configurations. The primary design consideration shifts toward balancing security enhancement against reliability degradation and hardware overhead. In this sense, the feed-forward depth serves as a tunable parameter enabling application-specific optimization.

4.2. Bias

Bias characterizes the distribution of bits "1" and "0" in PUF responses. Its ideal value is 50%, indicating uniform distribution of "1"s and "0"s, which maximizes unpredictability against attackers. Bias is quantified using the Hamming Weight (HW), calculated as follows:

$$HW(R) = \frac{1}{n}\sum_{i=1}^{n} R_i \times 100\% \tag{9}$$

where n is the number of stages in the PUF response, and R_i denotes the i-th bit of R.

In the experimental phase, 100 instances of 64-stage PUFs across 10 FPGA development boards were tested at room temperature. Each PUF received 50,000 challenges, generating a total of 500,000 response bits per FPGA board.

Figure 10 reveals the impact of varying FF stages on output randomness: as the number of FF stages increases, the distribution of response bits asymptotically approaches the ideal probability distribution (50%). However, the magnitude of optimization exhibits convergence characteristics. Data trends indicate that with three FF stages, the output uniformity is improved.

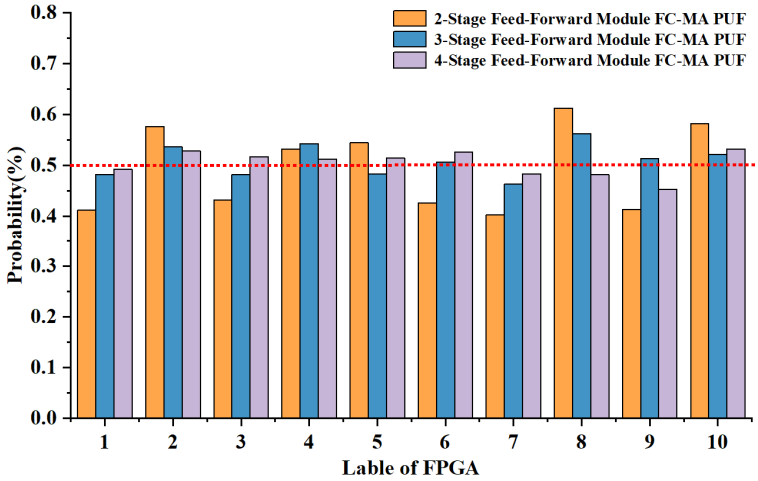


Figure 10. Bias Characteristics of FC-MA PUF Structures with Varying Numbers of Feed-Forward Units.

To further evaluate the quality of the generated responses, the bias of the PUF was also assessed under different feed-forward configurations. The measured mean bias values were 53.52%, 48.85%, and 49.88%, respectively. Among these, the selected 4-stage FC-MA PUF architecture exhibits a bias of 49.88%, which is very close to the ideal value of 50%, further confirming its well-balanced response distribution.

4.3. Uniqueness

The uniqueness metric quantifies the ability of different PUF instances to generate unique responses to identical challenges under the same environmental conditions. Its theoretical optimal value is a 50% Hamming distance between any two responses, as expressed in Equation (10):

$$Uniqueness = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{HD(R_i, R_j)}{n} \times 100\% \quad (10)$$

where k is the number of PUF instances and R_i and R_j are the responses derived from different PUF instances with the same challenge.

Ten areas were selected across 10 FPGA boards to deploy PUF circuits, resulting in 100 FC-MA PUF instances. Each PUF structure was tested with 10,000 randomly selected challenges. According to Equation (10), the inter-device Hamming distance distribution under room temperature and nominal voltage conditions is shown in Figure 11. FC-MA PUFs with varying numbers of FF modules exhibit near-normal distributions, with mean values of 55.52%, 51.21%, and 49.68%, respectively.

To further assess the statistical robustness of the reported results, confidence interval analysis was performed for the 4-stage configuration. A total of 100 independent instances were evaluated across 10 FPGA boards. The measured uniqueness is 49.68% with a standard deviation of 1.2%, resulting in a standard error of 0.12% and a 95% confidence interval

of 49.68% ± 0.24%. The bias is 49.88% with a standard deviation of 3.2%, yielding a 95% confidence interval of ±0.63%. The measured BER is 0.018% with a standard deviation of 0.006%, corresponding to a 95% confidence interval of 0.018% ± 0.0012%. These narrow confidence bounds suggest a relatively stable statistical behavior under the current sample size.

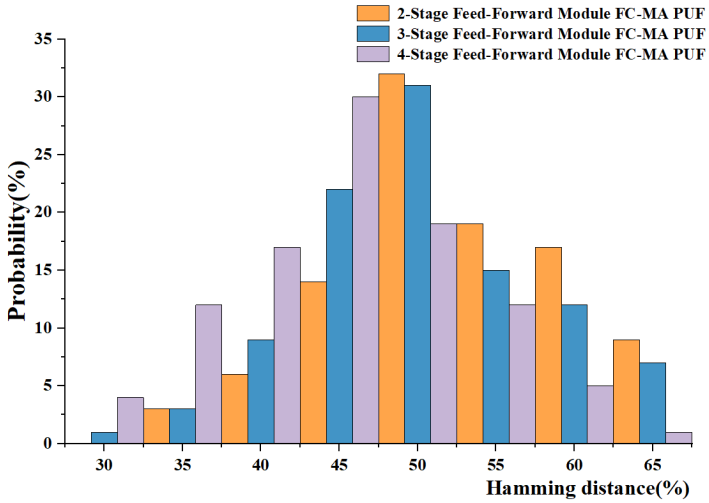


Figure 11. Uniqueness Characteristics of FC-MA PUF Structures with Varying Numbers of Feed-Forward Units.

4.4. Randomness Evaluation

To evaluate the statistical properties of the generated bitstreams from the proposed FCMA PUF and validate the static data quality of the FCMA PUF, this study employed the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-22 test suite for analysis. The experiment implemented 3FF FCMA PUF instances on 20 FPGA chips and evaluated 10 K-bit responses from each chip. According to the NIST standard, at a 99% confidence level, a *p*-value greater than 0.01 is required to consider the source as random. The experimental results demonstrate that the total 10 M-bit random bitstream generated from the chips successfully passed all items in the NIST SP 800-22 test suite, with detailed results shown in Table 1.

Table 1. Test results of 64-stage FCMA PUF.

Test Description	CPS PUF (FPGA)	
	***p*-Value**	**Rate**
Approximate Entropy	0.623	20/20
Block Frequency	0.287	20/20
Cumulative Sums	0.122	19/20
FFT	0.419	20/20
Frequency	0.193	20/20
Longest Run	0.403	20/20
NonOverlap.Template	0.241	20/20
Overlap.Template	0.097	19/20
Rank	0.452	20/20
Runs	0.621	20/20
Serial	0.387	20/20
Universal	0.538	20/20
Random Excursions	Success *	
Random Excursions Variant	Success *	

* All sb-tests pass the minimum requirement.

4.5. Resistant to Machine Learning Attacks

This section employs four classical machine learning algorithms-LR [2], SVM [19], Covariance Matrix Adaptation Evolution Strategy (CMA-ES) [22], and DNN [23]—to assess the modeling-attack resistance of the FC-MA PUF. Among them, the DNN model is widely adopted to approximate complex nonlinear challenge–response mappings and is commonly used to represent modern deep learning-based modeling attacks on delay-based PUFs. Experiments were conducted on a 64-stage FC-MA PUF instance implemented on the Xilinx Artix-7 FPGA platform. A test set of 1,000,000 CRPs was randomly generated, with 70% used for training and 30% reserved for testing. Prediction accuracy was evaluated by adjusting the training set size. The LR, SVM, and DNN algorithms were implemented in Python 3.11, while CMA-ES was executed in MATLAB 2024b. All CRP data were stored in text files and imported into their respective environments for training and prediction.

All modeling attacks were conducted under a black-box setting using screened CRPs only, meaning the attacker has no access to the internal RSM flag or feed-forward signals. For DNN attacks, a fully connected neural network with three hidden layers (128–64–32 neurons) was employed, using ReLU activation and a sigmoid output layer. Training was performed with the Adam optimizer at a learning rate of 0.001, batch size of 1024, and 100 epochs, incorporating early stopping with a patience of 10 epochs. CMA-ES was configured with a population size $\lambda = 50$, initial step size $\sigma = 0.5$, and a maximum of 500 iterations. All experiments were repeated over three independent random seeds. The reported prediction accuracies represent the mean value, with a standard deviation below 1.2% across runs.

It is important to note that invasive probing and high-resolution side-channel analysis (e.g., power or EM leakage) are outside the scope of this study and remain subjects for future investigation. Therefore, the following results focus exclusively on the PUF's resistance to modeling attacks under this black-box assumption.

As shown in Figure 12, the number of FF modules significantly affects the PUF's resistance to modeling attacks. Specifically, LR and SVM exhibit relatively poor attack performance against this structure, indicating that the CRPs generated by the PUF lack linear separability and thus effectively resist such linearity-based modeling attacks. In contrast, DNN and CMA-ES demonstrate stronger attack capabilities, achieving prediction accuracies of 58.2% and 56.2%, respectively, when only two FF modules are used. In particular, the DNN-based attack represents a powerful deep learning modeling approach capable of capturing complex nonlinear relationships between challenges and responses, highlighting the increased threat posed by nonlinear modeling techniques to this PUF architecture.

However, when the number of FF modules increases to four, the prediction success rates of all four attack methods drop to below 53%, which is close to the random guessing baseline of 50%. This result indicates that increasing the number of FF modules significantly enhances the PUF's resistance to machine learning–based modeling attacks.

Although the CMA-ES accuracy remains slightly above the ideal 50% random guessing rate, it is substantially lower than that observed in classical APUF and conventional feed-forward variants. Considering the million-scale CRP dataset used in our evaluation, a prediction rate close to 55% indicates that the attacker can only exploit limited residual structural information and fails to extract a stable, generalizable model. The slight deviation from 50% is attributable to the global optimization capability of CMA-ES, which may capture weak nonlinear correlations in the expanded path structure.

Further reduction toward the theoretical lower bound could be achieved by increasing the feed-forward depth, extending the overall stage count, or introducing more complex nonlinear combination strategies, such as multi-APUF parallel crossbar architectures. However, these enhancements must be carefully balanced against hardware overhead, FPGA symmetric layout constraints, and reliability degradation. Excessive structural complexity

may introduce additional delay variation and metastability risks, ultimately offsetting security gains. From a practical design perspective, increasing the number of feed-forward units provides a more efficient and controllable trade-off between modeling resistance and implementation cost.

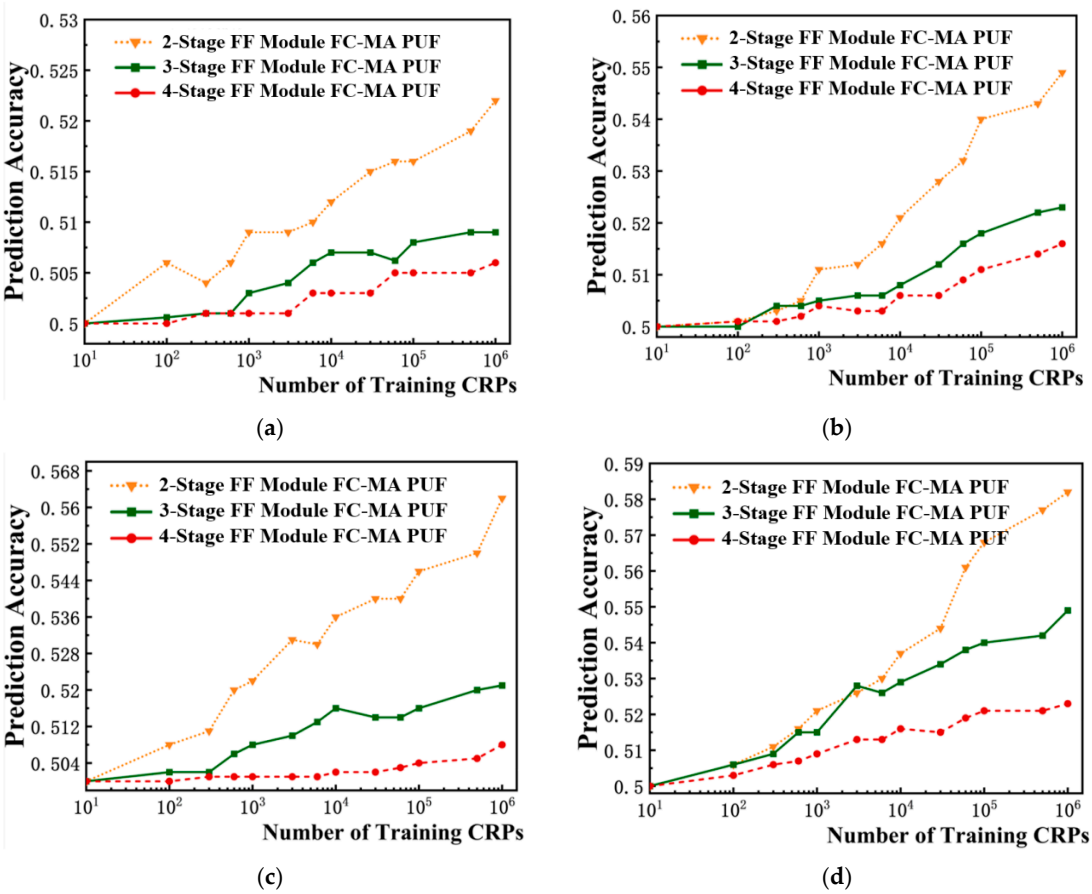


Figure 12. Prediction accuracy of ML attacks: (**a**) LR; (**b**) SVM; (**c**) DNN; (**d**) CMA-ES.

4.6. Structural Comparison

Table 2 compares the performance of different PUF Table 1 compares the performance of different PUF structures in terms of key metrics. By introducing a multi-stage feed-forward structure, the FC-MA PUF achieves significant optimization in bias rate and uniqueness, with the 3-stage flip-flop version reaching 48.85% bias rate and 51.21% uniqueness, approaching the ideal value of 50%. This performance not only surpasses that of the C-MA PUF (54.49% bias rate, 51.52% uniqueness), but is also comparable to the more resource-intensive 3-row XOR flip-flop 3-loop PUF (49.97% bias rate, 49.99% uniqueness). In terms of reliability, the FC-MA PUF maintains a bit error rate in the range of 10^{-5}~10^{-3}, significantly lower than the structure reported in the literature [12]. As the number of feed-forward modules increases, the bit width of the control signal S increases accordingly, introducing more cross-stage structures, which leads to a rise in hardware overhead with the number of flip-flop stages. The 3-stage feed-forward module requires 562 LUTs and 144 FFs, yet remains lower than the 8-row flip-flop XOR PUF in the literature [24]. Regarding resistance to modeling attacks, the prediction accuracy of the FC-MA PUF continues to decline as the number of feed-forward stages increases, dropping to 50.96–54.91% for all algorithms in the 3-stage module, comprehensively outperforming the C-MA PUF (55.33–56.70%). If the critical signal S of the C-MA PUF is leaked, its prediction accuracy rises to 92.42–97.73%, significantly reducing its defense capability. In contrast,

all feed-forward signals of the FC-MA PUF are generated internally in real time, eliminating the risk of leakage. Additionally, the anti-modeling performance of the 4th-order feed-forward module FC-MA PUF is comparable to the resource-intensive structure in the literature [25]. In summary, through its scalable feed-forward module architecture, the FC-MA PUF can achieve an optimal balance among randomness, uniqueness, and attack resistance according to requirements, providing a solution for resource-efficient high-performance PUF design.

Table 2. The Comparisons of FC-MA PUF With Existing Solutions.

PUF Type		Bias	Uniqueness	BER	Hardware Overhead	Prediction Accuracy			
						LR	SVM	CMA-ES	DNN
FC-MA PUF	2-Stage Feedforward	53.52%	55.52%	0.001%	462 LUTs and 124 FFs	52.21%	54.49%	58.20%	56.24%
	3-Stage Feedforward	48.85%	51.21%	0.004%	562 LUTs and 144 FFs	50.96%	52.36%	54.91%	52.12%
	4-Stage Feedforward	49.88%	49.68%	0.018%	674 LUTs and 172 FFs	50.64%	51.58%	52.33%	50.86%
C-MA PUF [12]		54.49%	51.52%	1.01%	508 LUTs and 98 FFs	55.33%/ 92.42% *	55.49%/ 93.28% *	56.70%/ 97.73% *	56.20%/ 94.10% *
3-row XFeed 3-loop PUF [13]		49.95%	49.93%	23%	853LUTs and 164 FFs	-	-	-	≈66.02%
3-row XOR FF 3-loop PUF [13]		49.97%	49.99%	21%	853LUTs and 164 FFs	-	-	-	≈77.21%
8-row FFXOR PUF [24]		49.77%	49.97%	0.007%	1400LUTs and 225 FFs	≈50%	-	≈50%	≈50%
BF PUF [25]		-	49.99%	0.22%	405LUTs and 312 FFs	Max = 52.60%			
(64,4)-cSOI PUF [26]		≈50%	49.8%	17%	1035 LUTs and 264 FFs	-	-	49.94%	50.55%

* Prediction accuracy when *S* is leaked.

Author Contributions: Conceptualization, X.Y.; Funding acquisition, Y.Z.; Investigation, X.Y. and C.Z.; Methodology, X.Y.; Supervision, Y.Z.; Validation, X.Y. and H.W.; Original draft writing, X.Y., C.Z.; Review and editing, X.Y., C.Z., H.W., and Y.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Joint Funds of the Natural Science Foundation of Hubei Province, China (Grant No. 2025AFD029), the Natural Science Foundation of Hubei Province, China (Grant No. 2024AFB876), and the Major scientific and technological project of Shenzhen (No. KJZD 20230923114611023).

Data Availability Statement: The data are not publicly available due to privacy or ethical restrictions.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Pappu, R.; Recht, B.; Taylor, J.; Gershenfeld, N. Physical one-way functions. *Science* **2002**, *297*, 2026–2030. [CrossRef] [PubMed]
2. Rührmair, U.; Sehnke, F.; Sölter, J.; Dror, G.; Devadas, S.; Schmidhuber, J. Modeling attacks on physical unclonable functions. In Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS), Chicago, IL, USA, 4–8 October 2010; pp. 237–249.
3. Lin, Y.; Liao, Y.; Wei, Y.; Zeng, W.; Erkan, U.; Toktas, A.; Zhang, Y.; Chen, D. Lightweight image encryption via four-dimensional Hénon memristor map and fast block permutation. *Nonlinear Sci. Control Eng.* **2025**, *1*, 025390012.
4. Lin, Y.; Liao, Y.; Zeng, W.; Wei, Y.; Chen, D.; Yuan, X.; Li, Y.; Erkan, U.; Toktas, A.; Zhang, C.; et al. 3D Non-degenerate Hyperchaos: Design, Analysis, and Application in Image Encryption. *IEEE Trans. Consum. Electron.* **2026**, *PP*, 1. [CrossRef]
5. Li, H.; Jin, Y.; Han, K.; Yu, D. A Lightweight XOR-PUF Structure for Resource Constrained Smart Device. In Proceedings of the 2019 IEEE 8th Global Conference on Consumer Electronics (GCCE), Osaka, Japan, 15–18 October 2019; pp. 168–169.

6. Sahoo, D.P.; Mukhopadhyay, D.; Chakraborty, R.S.; Nguyen, P.H. A multiplexer-based arbiter PUF composition with enhanced reliability and security. *IEEE Trans. Comput.* **2018**, *67*, 403–417. [CrossRef]
7. Nguyen, P.H.; Sahoo, D.P.; Jin, C.; Mahmood, K.; Rührmair, U.; Van Dijk, M. The interpose PUF: Secure PUF design against state-of-the-art machine learning attacks. *IACR Cryptol. ePrint Archive* **2018**, *2018*, 350. [CrossRef]
8. Wang, Y.; Wang, C.; Gu, C.; Cui, Y.; O'Neill, M.; Liu, W. A generic dynamic responding mechanism and secure authentication protocol for strong PUFs. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2022**, *30*, 1256–1268. [CrossRef]
9. Ali, R.; Ma, H.; Hou, Z.; Zhang, D.; Deng, E.; Wang, Y. A Reconfigurable Arbiter MPUF With High Resistance Against Machine Learning Attack. *IEEE Trans. Magn.* **2021**, *57*, 3402007. [CrossRef]
10. Taneja, S.; Alioto, M. PUF architecture with run-time adaptation for resilient and energy-efficient key generation via sensor fusion. *IEEE J. Solid-State Circuits* **2021**, *56*, 2182–2192. [CrossRef]
11. Lai, X.; Jenihhin, M.; Selimis, G.; Goossens, S.; Maes, R.; Paul, K. Early RTL Analysis for SCA Vulnerability in Fuzzy Extractors of Memory-Based PUF Enabled Devices. In Proceedings of the IFIP/IEEE International Conference on Very Large Scale Integration—System on a Chip, Salt Lake City, UT, USA, 6–9 October 2020; pp. 16–21.
12. He, Z.; Zhang, J.; Zhu, X.; Luo, S.; Zhang, Z.; Huang, Z. A cross-matrix arbiter PUF with high reliability and ML-resistance for IoT device security. *Microelectron. J.* **2025**, *160*, 1879–2391. [CrossRef]
13. Idriss, T.; Gavin, A.; Gabales, A.; Idriss, H.; Bayoumi, M. Xfeed puf: A secure and efficient delay-based strong puf using cross-feed connections. In Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), Austin, TX, USA, 28 May–1 June 2022; pp. 461–465.
14. Ayling, A.; Avvaru, S.V.S.; Parhi, K.K. Not all feed-forward MUX PUFs generate unique signatures. In Proceedings of the IEEE Computer Society Annual Symposium on VLSI, Miami, FL, USA, 15–17 July 2019; pp. 43–48.
15. Avvaru, S.V.S.; Parhi, K.K. Effect of loop positions on reliability and attack resistance of feed-forward PUFs. In Proceedings of the IEEE Computer Society Annual Symposium on VLSI, Miami, FL, USA, 15–17 July 2019; pp. 366–371.
16. Hemavathy, S.; Bhaaskaran, V.S.K. Arbiter PUF—A Review of Design, Composition, and Security Aspects. *IEEE Access* **2023**, *11*, 33979–34004. [CrossRef]
17. Kumar, S.; Niamat, M. Machine Learning based Modeling Attacks on a Configurable PUF. In Proceedings of the NAECON 2018—IEEE National Aerospace and Electronics Conference, Dayton, OH, USA, 23–26 July 2018; pp. 169–173. [CrossRef]
18. Joachims, T. Making large-scale SVM learning practical. *Tech. Rep.* **1998**, *8*, 499–526.
19. Zalivaka, S.S.; Ivaniuk, A.A.; Chang, C.-H. Reliable and modeling attack resistant authentication of arbiter PUF in FPGA implementation with trinary quadruple response. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 1109–1123. [CrossRef]
20. Wu, L.; Hu, Y.; Zhang, K.; Li, W.; Xu, X.; Chang, W. FLAM-PUF: A Response–Feedback-Based Lightweight Anti-Machine-Learning-Attack PUF. *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.* **2022**, *41*, 4433–4444. [CrossRef]
21. Becker, G.T. On the pitfalls of using arbiter-PUFs as building blocks. *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.* **2015**, *34*, 1295–1307. [CrossRef]
22. Hansen, N.; Müller, S.D.; Koumoutsakos, P. Reducing the Time Complexity of the Derandomized Evolution Strategy with Covariance Matrix Adaptation (CMA-ES). *Evol. Comput.* **2003**, *11*, 1–18. [CrossRef] [PubMed]
23. Avvaru, S.S.; Zeng, Z.; Parhi, K.K. Homogeneous and heterogeneous feed-forward XOR physical unclonable functions. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 2485–2498. [CrossRef]
24. Wang, H.; Hao, W.; Tang, Y.; Zhu, B.; Dong, W.; Liu, W. Deep neural network modeling attacks on arbiter-PUF-based designs. *Cybersecurity* **2025**, *8*, 11. [CrossRef]
25. Huang, Z.; Zeng, F.; Chi, Y.; Lin, Y.; Lu, Y.; Liang, H.; Bian, J.; Ouyang, Y.; Ni, T.; Wen, X. BF PUF: A Modeling Attack-Resistant Strong PUF Based on Bent Functions. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2025**, *33*, 2299–2311. [CrossRef]
26. Xu, C.; Zhang, L.; Mak, P.-I.; Martins, R.P.; Law, M.-K. Fully Symmetrical Obfuscated Interconnection and Weak-PUF-Assisted Challenge Obfuscation Strong PUFs Against Machine-Learning Modeling Attacks. *IEEE Trans. Inf. Forensics Secur.* **2024**, *19*, 3927–3942. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.