electronics

MDPI

Article

Variation-Resilient Low-Cost PUF with Trust-Based Authentication Implemented in 16 nm FinFET for IoT Security

Ching-Che Chung [1], Wei-Chia Huang [1] and Duo Sheng [2,*]

[1] Department of Computer Science and Information Engineering, National Chung Cheng University, Chia-Yi 621301, Taiwan; wildwolf@cs.ccu.edu.tw (C.-C.C.); karta3453824@gmail.com (W.-C.H.)
[2] Department of Electrical Engineering, National Taiwan University of Science and Technology, Taipei 106335, Taiwan
* Correspondence: duosheng@mail.ntust.edu.tw

Abstract

Physical Unclonable Functions (PUFs) generate unique chip identifiers from manufacturing variations, but transmissions over public networks can be exploited through eavesdropping. To improve variation resilience, the proposed SRPFD-PUF employs bit self-test (BST) for stable-CRP selection, while response-bit tolerance is considered in an illustrative authentication flow. By minimizing additional circuit overhead, strong baseline PUF metrics are maintained at low hardware cost, supporting integration in Internet of Things (IoT) devices. An illustrative PUF-based authentication flow is presented to demonstrate a potential IoT application; end-to-end protocol implementation and security validation remain outside the scope of this study. The three-condition BST screen yields a minimum simulated logarithmic reliability score of 98.93% under the evaluated PVT conditions within 0.675–1.05 V and −40–150 °C. With the circuit architecture and LFSR configuration disclosed, the evaluated machine-learning attacks yield prediction accuracies of 47.68–52.46%, indicating resistance to the tested modeling methods. The TSMC 16 nm FinFET physical design occupies 0.0117 mm^2, while post-layout simulation estimates 0.3089 mW at 100 MHz; no fabricated-silicon measurements are reported.

Keywords: Physically Unclonable Function (PUF); trust-based authentication; reliability; Internet of Things (IoT); machine learning resistance

1. Introduction

The Internet of Things (IoT) has become a fundamental component of modern life by enabling seamless information exchange among interconnected devices, including servers, smartphones, appliances, vehicles, and other equipment [1]. Before communication over public networks, authentication is required to grant access rights to IoT devices [2]; without such protection, vulnerability to malicious attacks and data manipulation is increased [3]. Physical Unclonable Function (PUF) technology has been widely adopted for identity verification, data encryption, and key generation in zero-trust environments [4–6]. Unique silicon fingerprints are produced by exploiting intrinsic manufacturing variations, such that distinct responses are generated even for chips sharing identical layouts when the same challenge is applied, thereby supporting device-level uniqueness.

PUF-based authentication between IoT devices and servers is commonly implemented in two stages. During enrollment, a trusted third party applies a set of challenges to the device and stores the corresponding responses as Challenge–Response Pairs (CRPs) in a protected server database for subsequent verification. During authentication, a challenge is

Check for updates

Academic Editor: Andrea Ballo

Received: 15 September 2026
Revised: 29 October 2026
Accepted: 2 November 2026
Published: 5 November 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.

transmitted from the server to the device-embedded PUF, the corresponding response is generated and returned, and the received response is compared with the enrolled CRPs to determine whether authentication has succeeded [7]. The overall interaction model is illustrated in Figure 1.

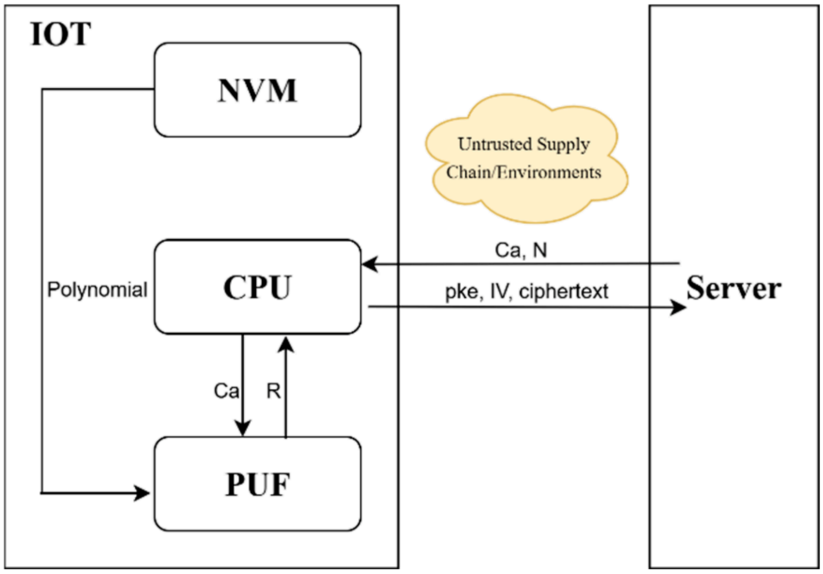


Figure 1. Block diagram of IoT device using PUF for the proposed protocol.

Several critical metrics are widely used to assess the quality and robustness of PUF architectures [8,9], including uniformity, reliability, uniqueness, and resistance to machine learning attacks. Uniformity evaluates the balance between logic-0 and logic-1 bits in PUF responses and is quantified by the Hamming weight $HW(R)$ and the probability P_1, as defined in Equations (1) and (2), respectively. In Equation (1), R denotes an N-bit PUF response, N represents the response length, and r_i denotes the i-th bit of R, where $r_i \in \{0, 1\}$. $HW(R)$ represents the Hamming weight of R, defined as the total number of logic-1 bits in the response. In Equation (2), P_1 represents the average percentage of logic-1 bits across K PUF responses, where K is the total number of evaluated responses, R_j denotes the j-th N-bit response, and $HW(R_j)$ represents its Hamming weight. Ideally, P_1 should be 0.5, indicating an equal distribution of logic-0 and logic-1 bits, while any deviation from this value indicates a bias in the PUF responses.

$$HW(R) = \sum_{i=1}^{N} r_i \tag{1}$$

$$P_1 = \frac{1}{K} \sum_{j=1}^{K} \frac{HW(R_j)}{N} \tag{2}$$

In addition to uniformity, output randomness can be further assessed using the NIST statistical test suite [10], which evaluates the generated bitstream against established randomness criteria. Reliability characterizes the stability of PUF responses under supply-voltage and temperature variations. In Equation (3), $S_{n,k,l}$ denotes the reliability score of the l-th response bit generated by the n-th PUF instance under the k-th challenge, where $p_{n,k,l}$ and $1 - p_{n,k,l}$ represent the probabilities of obtaining logic 1 and logic 0, respectively, under different operating conditions. In Equation (4), S_n represents the average reliability score of the n-th PUF instance, calculated by averaging $S_{n,k,l}$ over K challenges and L response bits, where K and L denote the total number of evaluated challenges and the number of response bits per challenge, respectively. Ideally, S_n approaches 1, indicating highly stable

responses. Reliability can also be evaluated using the Hamming Distance (HD)-based metric in Equation (5), where R represents the reliability expressed as a percentage, R_{ref} denotes the reference response obtained under nominal operating conditions, and R_i represents the response obtained in the i-th evaluation under different process, voltage, and temperature (PVT) conditions for the same PUF instance. Here, HD denotes the number of differing bits between two responses, n represents the response length in bits, m denotes the total number of PVT response observations compared with the reference response, and i is the comparison index.

$$S_{n,k,l} = 1 + log_2 \max\left(p_{n,k,l}, 1 - p_{n,k,l}\right) \tag{3}$$

$$S_n = \frac{1}{K \times L} \Sigma_{k=1}^{K} \Sigma_{l=1}^{L} S_{n,k,l} \tag{4}$$

$$R = \left(1 - \frac{1}{m} \Sigma_{i=1}^{m} \frac{HD\left(R_{ref}, R_i\right)}{n}\right) \tag{5}$$

Uniqueness measures the degree of variation among different PUF instances fabricated using the same circuit design. In Equation (6), U denotes the average pairwise HD-based uniqueness, expressed as a percentage, where m represents the total number of evaluated PUF instances, and n denotes the response length in bits. R_i and R_j represent the responses generated by the i-th and j-th PUF instances, respectively, under the same challenge. Ideally, U approaches 0.5, indicating that approximately half of the response bits differ between distinct PUF instances, thereby demonstrating strong inter-device differentiation.

$$U = \frac{2}{m(m-1)} \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} \frac{HD\left(R_i, R_j\right)}{n} \tag{6}$$

The primary contributions of this paper can be summarized as follows:

1. High-performance PUF architecture: The proposed SRPFD-PUF demonstrates favorable uniformity, reliability, configuration-dependent response diversity, and resistance to the evaluated machine-learning attacks. This demonstrates the effectiveness of the SRPFD-based design in addressing long-standing limitations of conventional PUF architectures. The circuit-level contribution lies in replacing the conventional DFF arbiter with an SR-latch-based PFD and integrating stable-CRP selection with bounded response-feedback challenge modification, evaluated using 16 nm FinFET post-layout Monte Carlo SPICE simulations.
2. Illustrative authentication application: A trust-based device–server exchange is outlined to illustrate the use of enrolled SRPFD-PUF responses in IoT authentication; a complete authenticated protocol has not been implemented or experimentally validated. The illustrative flow combines encrypted response transmission, response feedback, and single-use enrollment challenges, while the estimated 99.999% legitimate-device acceptance probability is an independent-bit theoretical result rather than measured end-to-end protocol performance.
3. Variation-resilient design through hardware–software co-optimization: By incorporating a bit self-test mechanism to eliminate CRPs with excessively small phase differences and employing an SR-latch-based Phase Frequency Detector (SRPFD) to reduce the dead zone of the sampling circuit, the proposed design achieves robustness against process and environmental variations. Furthermore, response-bit tolerance in the illustrative authentication flow offers a means of accommodating residual response errors, subject to future end-to-end validation. Compared to the conventional DFF-based arbiter PUF, the SR-latch-based PFD significantly enhances reliability with negligible additional hardware cost, making it highly suitable for resource-constrained IoT devices.

The remainder of the paper is organized as follows: Related work on PUF architectures is reviewed in Section 2, the proposed SRPFD-PUF architecture is described in Section 3, the authentication process is presented in Section 4, experimental results are reported in Section 5, and conclusions are provided in Section 6.

2. Related Work

PUFs are commonly categorized according to the correlation between CRPs and input challenge bits, and are generally classified as weak [3,10–13] or strong [14–17]. For strong PUFs, an exponential growth in CRPs with respect to challenges enables generation of many CRPs, which supports lightweight authentication [18–20] but also increases vulnerability to attacks based on CRP collection and machine learning modeling. By contrast, weak PUFs provide only a limited number of CRPs and are often used as replacements for keys stored in Read-Only Memory (ROM) or Non-Volatile Memory (NVM), supporting secure on-device key generation in IoT devices.

Many PUF architectures have been reported to improve reliability, randomness, and resistance to modeling attacks. In [21], a high-reliability ring oscillator (RO)-based PUF is presented that quantifies the delay of a time-to-digital converter (TDC) component; selection of an oscillation path with a larger frequency difference between upper and lower paths improves reliability relative to conventional implementations. In [17], the Delay Difference Quantization APUF (DDQ-APUF) adopts an arbiter-PUF architecture comprising 13 sets of delay cell chains used to quantify delay differences between adjacent paths, thereby producing 14 distinct outputs; although the circuit implementation differs from that of [16], the underlying concept remains largely similar. To mitigate bit flips induced by environmental variations, a fault-tolerance threshold is introduced, allowing authentication to succeed when the number of flipped bits remains within the threshold, which improves response stability and avoids discarding CRPs under varying operating conditions. FLAM-PUF [9] employs cycle-by-cycle response feedback to reconfigure its LFSR, whereas the proposed design retains the configured LFSR polynomial and uses internal feedback responses to modify eight predetermined challenge bits before generating the final response. While the bit-self-test arbiter PUF in [16] uses reliability flags to select stable CRPs, the present design additionally reduces the sampling dead zone using an SR-latch-based PFD and applies response-dependent challenge modification for modeling resistance.

In [19], a Genuine SPUF^{G} and a fake SPUF^{F} are combined to confuse attackers, reducing the usefulness of collected data for machine learning attacks; however, resetting the PUF circuit can shorten the duration of false responses and enable capture of additional genuine data, and exposure of NVM values can reveal the timing of genuine responses and weaken security. In [20], a Dynamic Challenge Transformation (DCT) protocol is introduced for strong PUFs, in which a Linear Feedback Shift Register (LFSR) is used in conjunction with a weak PUF to obfuscate the input challenge; dynamic alteration of the LFSR output produces diverse input–output mappings, but reliance on a weak PUF can compromise overall reliability. In [22], the Nonmonotonic Response Quantization PUF (NMQ PUF) strengthens resistance to machine learning attacks by using multiple ring oscillators and counters to generate nonlinear responses; nevertheless, increased structural complexity can adversely affect reliability, and effective server-side verification of source legitimacy during replay attacks is not supported. In [23], the obfuscated-interconnection PUF is proposed to enhance randomness and security through a fully symmetric design with symmetrically configured delay elements and interconnect structures, increasing the number of possible interconnections by a factor of 20 and improving resistance to machine learning attacks. In [24], an authentication mechanism for a DRAM PUF is proposed in which a software model is built on the server during registration; during authentication, the device ID is

transmitted to request a challenge and nonce, and the PUF response with related data is encrypted using the public key of the server for subsequent decryption and verification, thereby using asymmetric encryption to reduce susceptibility to man-in-the-middle attacks.

Despite significant advances in PUF research, existing designs still exhibit inherent trade-offs among reliability, security, resistance to machine-learning attacks, and implementation cost. To address these limitations, this paper presents a variation-resilient and cost-efficient SRPFD-PUF together with a lightweight authentication protocol. Unlike prior approaches that enhance security at the expense of reliability or hardware overhead, the proposed SRPFD-PUF simultaneously improves reliability, machine-learning resistance, and implementation efficiency. By employing an SR-latch-based phase-frequency detector to mitigate the dead-zone issue and a lightweight challenge-feedback mechanism to obfuscate CRP relationships without requiring a dedicated TRNG within the SRPFD-PUF circuitry or complex circuit structures, the proposed architecture achieves an excellent balance among reliability, security, randomness, and hardware cost. Furthermore, the proposed authentication protocol conceals PUF responses during transmission and uses single-use enrolled challenges to limit replay of previously recorded responses, supporting low-overhead authentication for resource-constrained IoT devices.

3. The Proposed SRPFD-PUF Circuit

The SRPFD-PUF, as shown in Figure 2, incorporates a feedback-based mechanism that exploits the inherent unpredictability of the PUF to further obfuscate data. By transforming the original challenge-response pairs, resistance against machine learning attacks is significantly enhanced.

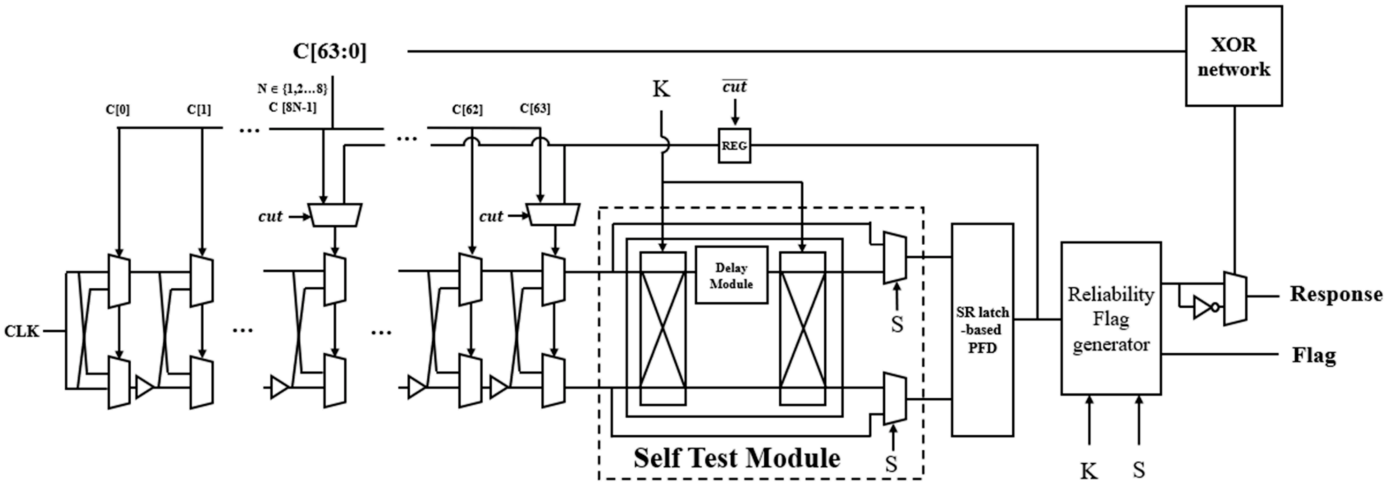


Figure 2. The circuit of SR-latch based PFD (SRPFD) PUF.

As illustrated in Figure 2, the proposed SRPFD-PUF generates a single-bit response from a 64-bit input challenge through four operational phases controlled by the signals *cut*, *S*, and *K*. Initially, the challenge bits control the multiplexers in the upper and lower delay paths, determining the propagation routes of the input signals. Due to intrinsic manufacturing variations, the two paths exhibit different propagation delays, resulting in a difference in signal arrival times. In the first phase, when *cut*, *S*, and *K* are all set to 0, the circuit enters the response feedback mode to generate the corresponding feedback responses. In the second phase, the *cut* signal is asserted, and the circuit enters the response output mode. The generated feedback responses are stored and used to replace the 8th, 16th, 24th, 32nd, 40th, 48th, 56th, and 64th bits of the original challenge to regenerate the response. This feedback mechanism disrupts the direct relationship between challenge-

response pairs (CRPs), thereby enhancing resistance to machine learning attacks. During this phase, the upper- and lower-path signals bypass the self-test module and enter the SRPFD, which determines their relative arrival order to generate a single-bit response. The resulting response is subsequently processed by a challenge-controlled XOR network, which determines whether the response should be inverted to improve output uniformity. In the third phase, the *S* signal is asserted to enable the self-test mode, in which the upper-path signal (*up_signal*) passes through the delay module, and the resulting response is stored in the reliability flag generator. In the fourth phase, the *K* signal is asserted while the circuit remains in the self-test mode, allowing the lower-path signal (*down_signal*) to pass through the delay module. The resulting response is XORed with the previously stored response to generate the reliability flag (*Flag*). When the phase difference between the upper- and lower-path signals is sufficiently large and the responses generated through their respective delay modules are identical, *Flag* is set to 1, indicating a reliable CRP. Otherwise, *Flag* is set to 0, and the corresponding unreliable CRP is discarded. The intermediate feedback response used to modify the challenge is not independently screened by bit self-test; the reliability flag evaluates the final response after feedback-based challenge modification.

To enhance the reliability of bit self-test (BST) PUFs, an SRPFD is employed to reduce the sampling dead zone, thereby improving the consistency of PUF responses. The effects of manufacturing process variations are evaluated using the foundry-provided TSMC 16 nm FinFET statistical SPICE models. In this study, Model 1 denotes the nominal reference configuration, whereas Models 2–6 represent five distinct Monte Carlo process-variation realizations generated using the same statistical modeling framework. These realizations do not correspond to different process corners or independently defined device models; instead, they represent different sets of sampled device-parameter values, resulting in variations in circuit characteristics and PUF responses. For each fixed post-layout netlist, the same Monte Carlo realization is retained across voltage and temperature sweeps to evaluate environmental sensitivity under consistent process-variation conditions, without introducing additional transient-noise sources or stochastic repeated-read simulations. The DFF-based and SRPFD-based BST PUFs are evaluated using separate circuit netlists; therefore, the Monte Carlo model indices in the reliability comparison presented later in this section should not be interpreted as physically paired device instances. To assess the effectiveness of the SRPFD in improving BST PUF reliability, both designs are evaluated under extended voltage and temperature stress conditions. These conditions are intended to investigate reliability degradation under extreme environmental variations rather than represent the normal operating range of the proposed circuit.

The SRPFD illustrated in Figure 3 is a commonly used phase frequency detector in phase-locked loop (PLL) systems. In an arbiter PUF, the D flip-flop (DFF) used for sampling effectively operates as a phase detector. Owing to the characteristics of the SRPFD, improved reliability can be achieved in PUF sampling compared with designs that employ DFFs. Consequently, an arbiter PUF that adopts an SRPFD as the sampling circuit can achieve better reliability than conventional DFF-based implementations.

Tables 1 and 2 present simulated dead zones of the DFF and SRPFD under the same process node across different process variations, voltage, and temperature conditions. The evaluated scenarios exceed typical voltage and temperature ranges used in standard analyses in order to assess PUF behavior under harsh environmental conditions. Two observations can be drawn from the simulation results. Under identical conditions, the SRPFD exhibits a significantly smaller dead zone than the DFF. Under the same process variation and fixed voltage, the worst-case circuit performance does not necessarily occur at the highest temperature within the −40 °C to 150 °C range. This behavior can be attributed to the temperature inversion effect in 16 nm FinFET processes; however, the occurrence of this

effect depends on the specific standard cells used in the design. Accurate assessment of this effect requires circuit-level simulations and measurements.

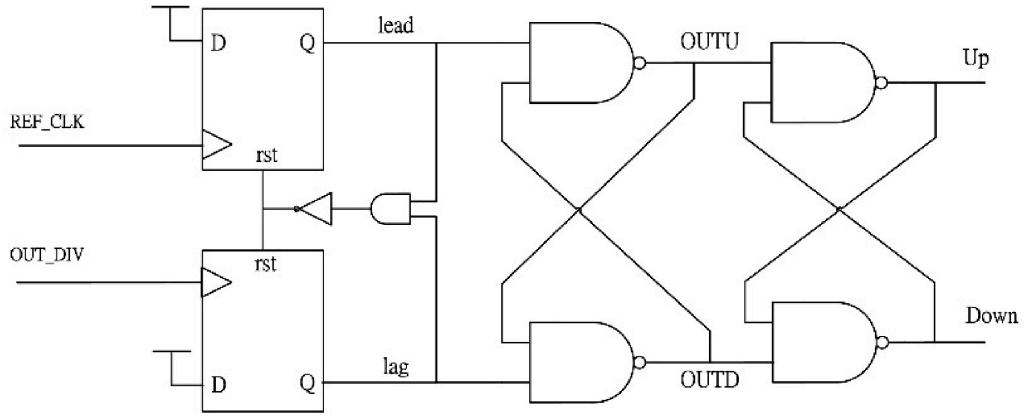


Figure 3. SR-latch based PFD.

Table 1. Dead zone of DFF setup time.

Dead Zone	Unit (ps)
(TT, 0.8 V, 25 °C)	7
(FF, 1.4 V, −40 °C)	4
(FF, 1.4 V, 150 °C)	7
(SS, 0.6 V, 150 °C)	26
(SS, 0.6 V, −40 °C)	38

Table 2. Dead zone of SR-latch based PFD setup time.

Dead Zone	Unit (ps)
(TT, 0.8 V, 25 °C)	1
(FF, 1.4 V, −40 °C)	0.5
(FF, 1.4 V, 150 °C)	0.5
(SS, 0.6 V, 150 °C)	4
(SS, 0.6 V, −40 °C)	8

As shown in Figure 4, the feedback mechanism is first removed to isolate reliability evaluation. The reliability values in Tables 3 and 4 are calculated using the Hamming-Distance-based metric in Equation (5), with the reference responses obtained at the nominal operating condition of 0.8 V and 25 °C. Table 3 reports reliability when the sampling circuit uses a DFF, whereas Table 4 reports reliability when an SRPFD is used. Both data sets are simulated over a voltage range of 0.625 V to 1.45 V and a temperature range from −40 °C to 150 °C. Among 20,000 simulated CRPs, approximately 15,500 exhibit the flag equal to 1. Reliability is calculated using CRPs with the flag equal to 1 under the (0.8 V, 25 °C) condition. Tables 3 and 4 therefore characterize feedback-disabled BST-PUF variants rather than the complete response-feedback circuit in Figure 2, and the Monte Carlo model indices are not physically paired between the two different circuit netlists.

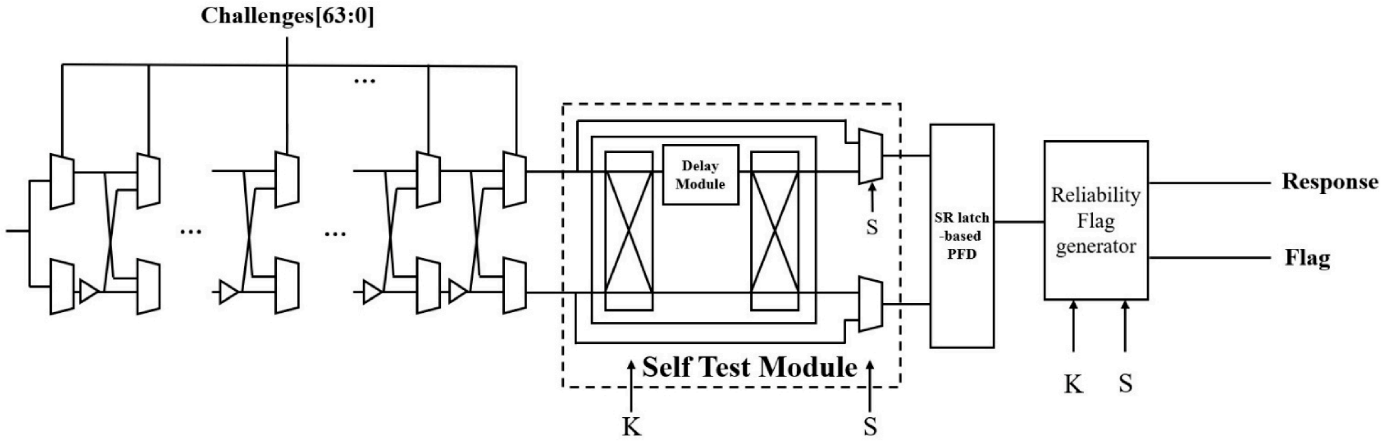


Figure 4. The circuit of BST PUF with SR-latch based PFD.

Table 3. Reliability of the BST PUF with DFF.

Delay Module	BUFFD20BWP7D5T20P96CPD
Monte Carlo	(0.8 V, 25 °C) (1.45 V, −40 °C) (0.625 V, −40 °C)
Model 2	0.7726
Model 3	0.7552
Model 4	0.6624
Model 5	0.9597
Model 6	0.9807

Table 4. Reliability of the BST PUF with SR-latch based PFD.

Delay Module	BUFFD20BWP7D5T20P96CPD
Monte Carlo	(0.8 V, 25 °C) (1.45 V, −40 °C) (0.625 V, −40 °C)
Model 2	0.9596
Model 3	0.9275
Model 4	0.9395
Model 5	0.9173
Model 6	0.9395

Due to page limitations, simulation results for all corner cases are not included. Because the temperature inversion effect prevents reliable prediction of the best- or worst-performing corner in advance, simulations are performed across all voltage and temperature combinations and the worst-case scenario is selected for comparison. Within the environmental variation range of 0.675 V to 1.05 V and −40 °C to 150 °C (the final operating range of the circuit), the minimum reliability increases from 99.94% to 99.97%, and the improvement is not explicitly tabulated because the change is marginal. Because both circuits are already highly reliable within 0.675 V to 1.05 V, the voltage sweep is extended to 0.625 V to 1.45 V as an exploratory stress comparison to reveal differences in sampling sensitivity, not as an additional intended operating range. As indicated by Tables 3 and 4, this wide voltage range can cause a substantial reliability drop for PUFs using a DFF as the sampling circuit (Model 4 minimum 66.24%). When an SRPFD is used, reliability also decreases under the widened range, but the minimum remains above 90% (Model 5 minimum 91.73%). The observed minimum reliability over these separate Monte Carlo samples increases from 66.24% with DFF sampling to 91.73% with SRPFD sampling under the extended stress conditions, without implying an improvement for every individual process realization.

4. Authentication Process of Proposed Protocol

The authentication flow in this section is an illustrative system-level application of the proposed SRPFD-PUF for resource-constrained IoT devices, rather than an implemented or experimentally validated end-to-end authentication protocol. The threat model considers an adversary capable of eavesdropping on, intercepting, modifying, and replaying communication messages. The adversary may also collect CRPs, obtain knowledge of the PUF architecture and challenge-generation parameters, and perform machine learning-based modeling attacks to predict PUF responses.

The security analysis assumes that device enrollment is performed in a trusted environment, the server's private key remains confidential, and the server's public key is securely provisioned to legitimate devices. The intrinsic manufacturing variations in the PUF are assumed to be difficult to reproduce. Disclosure of device-side configuration information, such as the LFSR seed and polynomial, is considered in the modeling-attack evaluation. However, invasive physical attacks, detailed side-channel attacks, and compromise of the server's private key are outside the scope of the present experimental evaluation. The analysis focuses on PUF response predictability, error-tolerant authentication probabilities, and the computational overhead of the cryptographic operations. Message integrity, replay prevention, and resistance to key compromise require additional protocol-level protections and validation.

A trust-based authentication protocol is proposed for SRPFD-PUF-based devices in which registration is performed using genuine CRPs and response values are concealed during transmission to prevent disclosure of correlations between CRPs. Rather than being transmitted directly, PUF-generated responses are encrypted prior to communication. The machine-learning evaluation considers an attacker who knows the SRPFD-PUF circuit architecture and LFSR configuration, rather than claiming resistance to all forms of reverse engineering. Under this assumption, the response-feedback mechanism is evaluated using observed final PUF responses, while device-specific internal feedback values are not directly exposed. The symbols used in this protocol are defined in Table 5.

Table 5. The Notation Definition for the Trust-based Authentication Protocol.

Notation	Length (Bits)	Description
i		The number of devices
ID_i		The one-time programmable (OTP_i) stores the identification number of devices.
Ca	64	A sequence of challenges generated by the challenge generator $LFSR_C$.
N	28	A 28-bit random number
pke	256	Public key corresponding to ske. Sent to the server to allow it to derive the same shared secret.
ske	256	Randomly generated per session. Used with pks to perform X25519 key exchange and derive the shared secret.
pks	256	Pre-generated and securely provisioned into the device. Used by the device for X25519 key exchange.
sks	256	Pre-generated and securely provisioned into the server. Used by the server for X25519 key exchange.

Table 5. *Cont.*

Notation	Length (Bits)	Description
IV	128	Random 16-byte value used in AES-CBC encryption to ensure ciphertext uniqueness.
ciphertext	128	The result of AES-CBC encryption over the original plaintext message.

4.1. Enrollment Phase

Public key cryptography relies on a mathematically linked key pair composed of a public key and a private key. Data encrypted with the public key can be decrypted only with the corresponding private key, and the inverse operation is also supported. In authentication protocols, this asymmetry is leveraged to establish trust between a device and a server, since sensitive data can be protected using the server's public key and recovered only by the server holding the private key.

The protocol is organized into enrollment and authentication stages. During the enrollment stage, as shown in Figure 5, each device is assigned a unique identifier and provisioned with the server's X25519 public key for secure authentication. Selected bits of the server public key directly configure the feedback polynomial of the PUF challenge-generator LFSR, while the enrollment challenge Ca provides its initial state for generating the corresponding challenge sequence. These values serve as configuration parameters for the CRP mapping rather than sources of cryptographic entropy. The PUF challenge generator does not require a primitive polynomial, and nondegenerate configurations capable of producing the required challenge sequence are used. For a given enrollment challenge Ca, an LFSR-generated candidate challenge sequence is processed through the PUF with response feedback until 100 stable response-bit positions are selected. Candidates with flag = 0 are excluded during enrollment, and the ordered indices of the 100 selected candidates must be preserved to maintain consistent response-bit positions during authentication. In a practical system integration, the index mapping associated with each enrollment challenge Ca and its LFSR configuration could be provisioned into integrity-protected device-side host NVM and reused by trusted firmware; this would incur additional firmware and NVM overhead and has not been implemented or verified in the present study. During enrollment, the server stores multiple distinct pairs of enrollment challenges Ca and their corresponding 100-bit responses for each device ID as reference CRPs for separate authentication sessions. Because enrollment can be conducted in a secure environment with physical access to the device, key provisioning can be performed directly without the need for a key exchange algorithm, improving both efficiency and security.

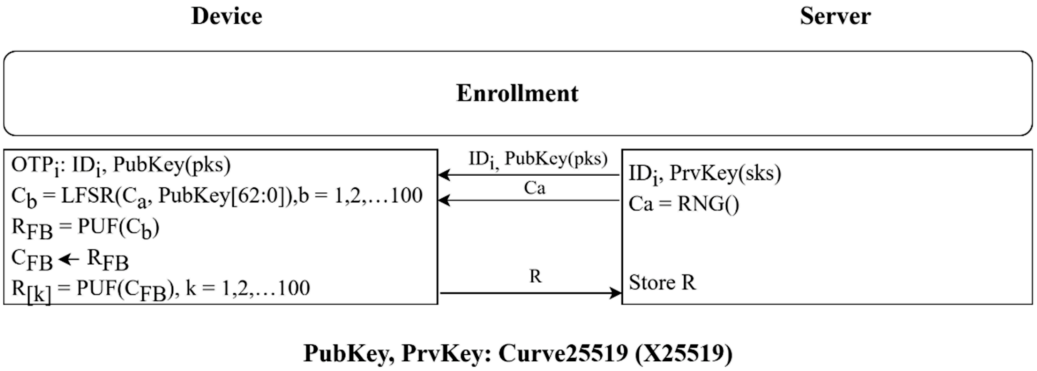


Figure 5. The enrollment phase of the trust-based authentication protocol.

4.2. Authentication Phase

During the authentication stage, as shown in Figure 6, the device first sends the assigned *ID* to the server. If the *ID* cannot be located, the process is terminated. Otherwise, the server selects a previously unused enrollment challenge Ca and its associated reference response for that device ID, and sends Ca together with a newly generated 28-bit nonce N. The selected Ca is reserved for one authentication session when issued and is never reissued, including after an unsuccessful or timed-out attempt. The server-side 28-bit nonce N is generated by an LFSR with a fixed primitive polynomial, providing a maximal-period deterministic sequence rather than cryptographically unpredictable random numbers. Nonce values are not assumed to remain unique after LFSR reinitialization, including server restart, or across concurrent authentication sessions. For deployment, the server must preserve the issued-challenge records across restarts and ensure that concurrent sessions cannot reserve the same Ca; any issued Ca remains retired even after authentication rejection, failure, or timeout. Mitigation of finite enrolled-CRP pool exhaustion requires application-dependent capacity planning and server-side issuance controls, such as rate limiting, one pending request per device ID, and temporary suspension after repeated failures or timeouts; these controls have not been implemented or evaluated in this study. Secure re-enrollment can replenish CRPs for serviceable devices but cannot be assumed for inaccessible deployed sensors, whose enrolled-CRP capacity must be planned for a finite intended service lifetime.

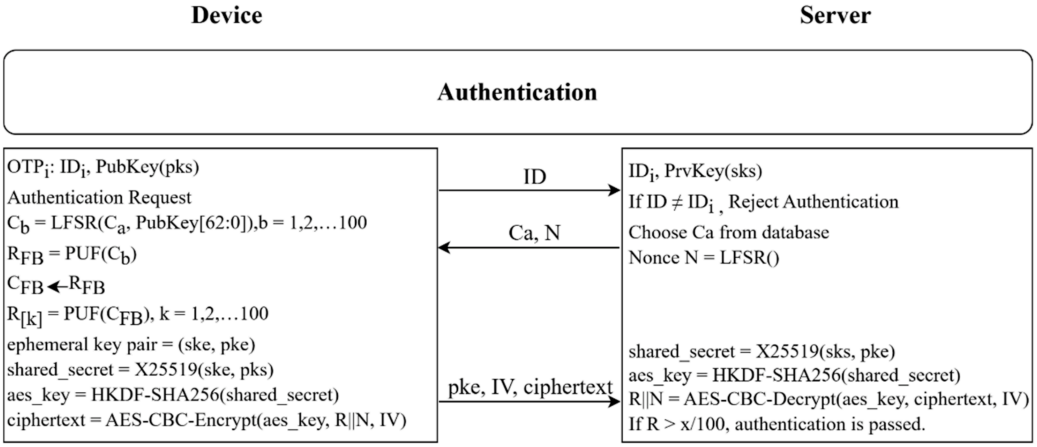


Figure 6. The authentication phase of the trust-based authentication protocol.

After receiving *Ca* and *N*, the device would regenerate the enrolled 100-bit response using the same LFSR configuration and the previously provisioned candidate indices, rather than selecting positions again from the run-time BST flags. The regenerated response is concatenated with the 28-bit random number *N* to form a 128-bit message. For secure transmission, a fresh ephemeral key pair (*ske*, *pke*) is generated per session, and an X25519 key exchange is performed with the server's preloaded public key *pks* to derive a shared secret. The standard X25519 Diffie-Hellman mechanism is followed, which is widely adopted for secure key establishment in modern protocols. The 128-bit message is then encrypted using AES in CBC mode, and the tuple {*pke*, *IV*, *ciphertext*} is transmitted to the server. The device-side X25519 ephemeral private key and AES-CBC IV are assumed to be generated using a cryptographically secure random number generator (CSPRNG) initialized from a trusted entropy source on the IoT host platform. This platform-level requirement does not imply a dedicated TRNG in the SRPFD-PUF circuit and is not included in the reported PUF area and power results.

Upon receipt, the server uses the private key *sks* and the ephemeral public key *pke* to derive the same shared secret and to derive encryption keys via the hash-based key

derivation function (HKDF). The ciphertext is then decrypted with AES-CBC to recover the original message. The recovered 100-bit PUF response is compared with the enrolled reference associated with the current device ID and session-specific challenge Ca, and authentication is accepted only when the mismatch count is within the predefined tolerance.

AES-CBC is used to conceal the transmitted PUF response, but encryption in CBC mode does not by itself guarantee message integrity or detect deliberate ciphertext modification. The replay-related claim is limited to preventing the reuse of previously issued enrollment challenges through server-side challenge management. Protection against active modification of messages requires an additional authenticated communication mechanism beyond the scope of the present circuit-oriented evaluation.

For the proposed implementation, an X25519 key exchange using the ephemeral private key *ske* and the server's static public key *pks* is reported to require approximately 67 milliseconds on a 48 MHz ARM Cortex-M0 microcontroller based on publicly available implementations. Processing the derived shared secret with the HKDF requires less than 1 millisecond for a 256-bit input. After key derivation, encryption of a 128-bit message using AES in CBC mode takes about 0.2 milliseconds based on benchmark results from SharkSSL, which is a lightweight SSL/TLS stack optimized for resource-constrained embedded systems such as ARM Cortex-M0. Based on these publicly reported software benchmarks, the selected cryptographic operations have an illustrative combined execution-time estimate of approximately 68 milliseconds, rather than a measured end-to-end authentication latency. Although this execution time exceeds that of static shared-key methods, a fresh device-side ephemeral key pair is used to derive a session-specific encryption key. However, later compromise of the server's static private key would allow past shared secrets to be reconstructed from recorded device public keys; therefore, forward secrecy against this event is not provided. The additional computation may impact resource-constrained IoT devices; however, the design targets entry-level microcontrollers and performs authentication once at the start of communication. After successful authentication, data transmission continues without additional cryptographic overhead, minimizing any noticeable effect on communication latency.

5. Experimental Results

The layout of the SRPFD-PUF chip is shown in Figure 7. The SRPFD-PUF is implemented using the TSMC 16 nm FinFET process with standard cells. The core size is 250 μm × 250 μm, and the total chip area including I/O PAD is 510 μm × 510 μm. The active area is 0.0117 mm^2 (Interface area + LFSR area + SRPFD-PUF area + Controller area = 0.0040 mm^2 + 0.0040 mm^2 + 0.0029 mm^2 + 0.0008 mm^2 = 0.0117 mm^2). The power consumption in multi-bit output response mode is 0.3089 mW, and the maximum operating frequency is 100 MHz. Figure 7 presents the physical layout used for post-layout circuit simulation; no fabricated-silicon measurement results are reported.

5.1. Modes of Operation in the SRPFD-PUF Test Chip

Two modes of operation are supported by the SRPFD-PUF test chip. In single-bit mode, CRPs are collected for the evaluation of uniformity, reliability, and the accuracy of machine learning attacks, and for establishing a software model. In multi-bit mode, 100-bit responses are generated for evaluating configuration-dependent response diversity.

The timing diagram for the single-bit output response mode is illustrated in Figure 8. A 64-cycle initialization is performed for the seed and polynomial of the LFSR, and the ready signal is asserted after initialization. Each challenge (*challenges [63:0]*) generated by the challenge generator LFSR requires four cycles to produce a CRP pair. When the positive edge of the *grab* signal is triggered, the *response*, *response_fb*, and *flag* signals are

captured. These captured signals are used for PUF characterization and enrollment: the reliability flag screens unstable CRPs, whereas response_fb is an internal feedback value for subsequent challenge modification. In the normal authentication exchange of Figure 6, neither response_fb nor flag is transmitted as a protocol output, and the final PUF response is included in the encrypted message. Hardware or firmware mechanisms restricting access to characterization signals and test controls after deployment are outside the scope of this circuit-oriented evaluation.

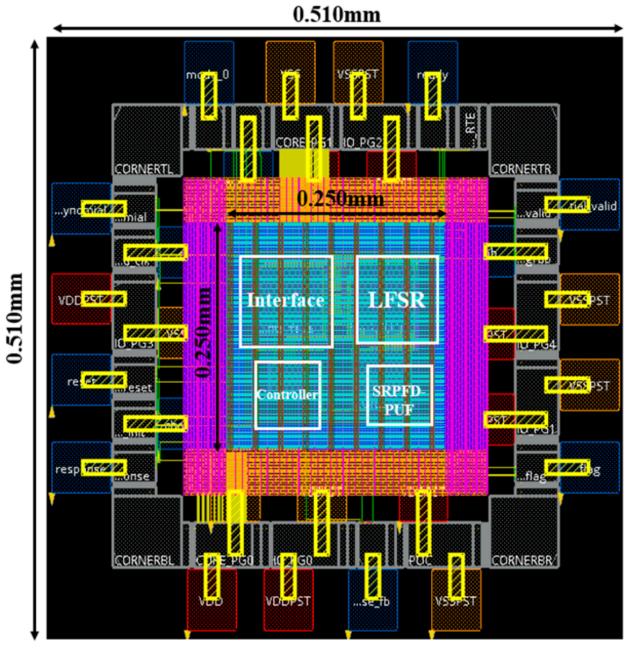


Figure 7. The layout of proposed SRPFD-PUF chip.

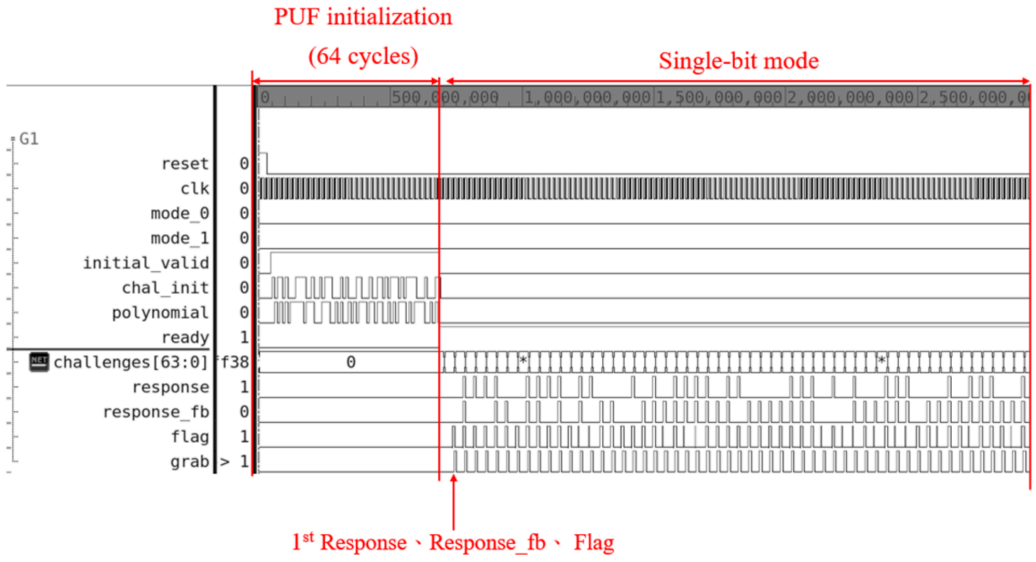


Figure 8. Timing diagram for single-bit output response mode.

The timing diagram for the multi-bit output response mode is illustrated in Figure 9. In the illustrated timing, 100 candidate bits require 400 cycles (100×4) if none is discarded. Rejected candidates (flag = 0) require additional cycles to obtain 100 stable response bits. Similar to the single-bit output response mode, a 64-cycle initialization of the LFSR is performed using a manually entered seed and polynomial. After the 100-bit response

is generated, the *Initial_valid* signal is asserted again. By manually inputting different seeds and polynomials to reinitialize the circuit, additional sets of multi-bit responses can be obtained.

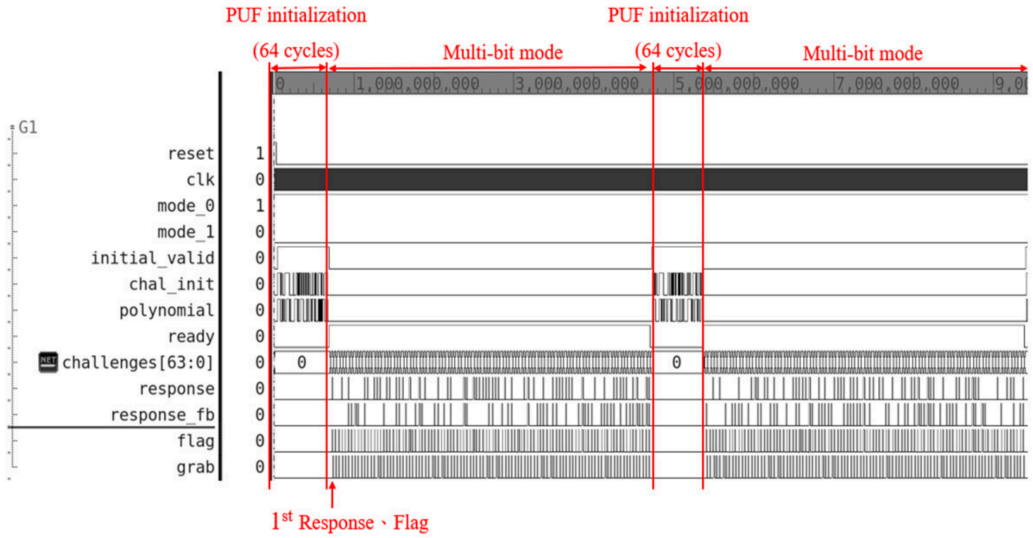


Figure 9. Timing diagram for multi-bit output response mode.

5.2. Simulation Results and Performance Evaluation of the SRPFD-PUF

Monte Carlo SPICE simulations were performed to collect a large number of CRPs and to evaluate uniformity, configuration-dependent response diversity, machine-learning prediction accuracy, and reliability. Tables 6 and 7 report uniformity and response diversity at (0.675 V, 150 °C), (0.8 V, 25 °C), and (1.05 V, −40 °C), whereas Table 8 reports reliability at (0.675 V, −40 °C), (0.8 V, 25 °C), and (1.05 V, 150 °C), across five Monte Carlo process-variation realizations. In the TSMC 16 nm process, due to the temperature inversion effect, high-temperature and low-voltage conditions do not necessarily represent the worst-case scenario. To account for this effect, the reliability assessment also considered all four combinations of the voltage endpoints (0.675 and 1.05 V) and temperature endpoints (−40 and 150 °C), while the tables present selected conditions rather than a complete per-corner results matrix.

Table 6. Uniformity Post-layout Simulation Results.

Monte Carlo	(0.675 V, 150 °C)	(0.8 V, 25 °C)	(1.05 V, −40 °C)
Model 2	0.4998	0.4983	0.5012
Model 3	0.5021	0.4994	0.5006
Model 4	0.5023	0.5030	0.5021
Model 5	0.5034	0.5035	0.5032
Model 6	0.5040	0.5003	0.5033

Table 7. Response Diversity under Different LFSR Configurations and Process Variations (Post-Layout Simulation Results).

Monte Carlo	(0.675 V, 150 °C)	(0.8 V, 25 °C)	(1.05 V, −40 °C)
Model2	0.4922	0.4958	0.5008
Model3	0.4957	0.4974	0.5012
Model4	0.5014	0.5035	0.4922
Model5	0.4998	0.4913	0.4909
Model6	0.4917	0.4987	0.4971

Table 8. Reliability Post-layout Simulation Results.

Monte Carlo	(0.675 V, −40 °C), (0.8 V, 25 °C), (1.05 V, 150 °C)
Model2	0.9926
Model3	0.9943
Model4	0.9932
Model5	0.9893
Model6	0.9947

Uniformity was evaluated by simulating 10,000 CRPs under three temperature and voltage conditions. Based on the reliability signal *flag*, approximately 7500 stable responses were selected from the typical case (0.8 V, 25 °C) for analysis. This corresponds to approximately 75% retained responses (7500/10,000) and 25% discarded responses under nominal-condition screening. The post-layout simulation results are shown in Table 6. Good uniformity is achieved by employing an XOR network that randomly toggles the output responses based on the input challenge bits, and the uniformity consistently approaches the ideal value of 0.5 under different conditions. The selected NIST SP 800-22 statistical test results [10] of the post-layout simulation are summarized in Table 9, providing supplementary characterization of the PUF response bitstream. These statistical tests characterize the PUF response bitstream but do not establish its suitability as a cryptographic entropy source.

Table 9. The NIST Random Tests Results.

Statistical Test	*p*-Value	Results
Frequency	0.71	Pass
BlockFrequency	0.95	Pass
Runs	0.63	Pass
Serial	0.91	Pass
ApproximateEntropy	0.11	Pass
CumulativeSums (Forward)	0.35	Pass
CumulativeSums (Backward)	0.64	Pass

Configuration-dependent response diversity of the SRPFD-PUF was evaluated by initializing the LFSR with different seeds and polynomials. During simulation, 100-bit responses were collected for 16 simulated PUF configurations with different LFSR seeds and polynomials under the evaluated voltage and temperature conditions. The post-layout results in Table 8 show that the normalized response differences approach 50% under the evaluated configurations and operating conditions. These response-diversity results reflect both changes in LFSR seed/polynomial configurations and Monte Carlo process variations; they do not isolate conventional inter-device uniqueness under identical challenge sequences.

To further enhance reliability, the reliability signal *flag* was analyzed across multiple operating conditions. By selecting approximately 6000 stable responses that consistently maintained a logic-high *flag* under three distinct voltage-temperature conditions, improved reliability is demonstrated relative to the conventional approach of selecting CRPs only at 0.8 V and 25 °C. The approximately 6000 accepted responses were selected from 10,000 candidates, corresponding to 60% retention and 40% rejection. These results characterize PVT response stability conditional on the three-condition selection, whereas an additional fixed-index validation at PVT conditions excluded from screening is presented below; stochastic repeated-read noise was not evaluated. Under the conventional method, the minimum reliability is around 96% and the average is 96–97%, whereas the proposed selection method improves the worst-case reliability to nearly 99% and achieves an average consistently above

99%. Multi-PVT BST screening increases the enrollment effort, and the overall provisioning cost depends on the number of reliably screened CRP records required by the intended authentication frequency and service lifetime.

Table 9 summarizes the model-indexed logarithmic reliability scores obtained from the three-condition stable-CRP selection. The separately reported 99.35% mean is the equal-weight average of 20 unrounded scores from four distinct three-PVT screening scenarios (five Monte Carlo realizations each), with a separately selected stable-CRP set for each scenario; it is not the arithmetic mean of the five values in Table 9.

As a held-out PVT check using existing post-layout simulation responses, the CRP indices selected with BST flags at (0.8 V, 25 °C), (1.05 V, 150 °C), and (0.675 V, −40 °C) were fixed and evaluated at (1.05 V, −40 °C) and (0.675 V, 150 °C), without re-screening or replacement. The same challenge input sequence was used across PVT conditions; the reanalysis retained the original row correspondence, including repeated challenge entries. Across five Monte Carlo realizations and the two held-out conditions, the equal-case mean conservative failure rate, which includes unresolved output samples as failures, was 2.19% for three-condition selection compared with 5.05% for nominal-only selection (worst case: 4.38% for three-condition selection). These held-out results use nominal-reference Hamming-distance comparisons and are distinct from the logarithmic reliability scores in Table 9.

Machine-learning modeling resistance was evaluated for the complete SRPFD-PUF circuit in Figure 2 under an information-disclosure assumption in which the attacker knows the circuit architecture, LFSR seed and polynomial, and response-processing rules, and can collect final PUF responses to construct a CRP dataset. The device-specific internal feedback values (response_fb) are not assumed to be directly observable in this attack scenario. In Table 10, the prediction accuracies are reported for several commonly used machine learning attack models: MLP (Multi-Layer Perceptron), LR (Logistic Regression), SVM (Support Vector Machine), GB (Gradient Boosting), and CMA-ES (Covariance Matrix Adaptation Evolution Strategy), an evolutionary optimization-based approach. A total of 15,000 CRPs were simulated, and approximately 11,500 reliability-screened CRPs were retained for machine-learning evaluation. For each Monte Carlo realization, these samples were split into training (80%) and held-out testing (20%) subsets with a fixed data-partitioning seed of 42; MLP reserved an additional 20% of its training portion for validation, whereas LR employed five-fold cross-validation. The evaluated configurations included a two-hidden-layer MLP (32 and 16 units), an RBF-kernel SVM (C = 1), gradient boosting with 5000 estimators, and CMA-ES with a population size of 20. The reliability flag is used only to select stable CRPs and is not provided as an input feature to the machine-learning models. Exposure of device-side NVM configuration data is represented by the known LFSR parameters and does not imply firmware control or invasive access to internal feedback signals. As presented in Table 10, the prediction accuracy remains close to 50%, which is the ideal value achieved by the feedback mechanism.

Table 10. Accuracy of ML Attacks with Exposed Seed/Polynomial Post-Layout Simulation Results.

Monte Carlo (%)	**Post-Layout Simulation at (0.8 V, 25 °C)**				
Machine Learning	MLP	LR	SVM	GB	CMA-ES
Model 2	50.17	48.62	52.28	49.33	51.09
Model 3	47.88	51.71	49.56	48.75	50.41
Model 4	52.01	48.39	50.86	49.04	47.91
Model 5	49.77	51.38	48.12	50.65	52.46
Model 6	50.08	49.22	47.68	51.94	48.98

In an earlier circuit-level evaluation at (0.8 V, 25 °C), the SRPFD/BST-PUF baseline without response feedback yielded 100% prediction accuracy for both MLP and gradient boosting across Models 2–6 using approximately 16,000 reliability-screened CRPs. For the complete feedback-enabled architecture, prior simulation datasets containing approximately 16,000 and 110,000 screened CRPs, selected from 20,000 and 140,000 candidates, respectively, were evaluated, with prediction accuracies ranging from 47.12% to 52.34% for the larger dataset across five ML algorithms and five Monte Carlo models. These earlier circuit-level results are distinct from the post-layout evaluation in Table 10, and the comparison does not constitute a matched feedback-only ablation, a separate XOR-cancellation attack, or a multi-seed training-robustness assessment.

Table 11 is a comparison table summarizing the performance of different PUFs. As the compared designs use different technologies, implementation platforms, and evaluation conditions, Table 11 is intended as a representative literature overview rather than a matched ablation study or a direct performance ranking. In this work, extensive Monte Carlo simulations covering numerous combinations of process, voltage, and temperature (PVT) variations are performed. In particular, the proposed-work value of 49.66% in Table 11 reflects configuration-dependent response diversity with varying LFSR seeds/polynomials and process variations, rather than conventional inter-device uniqueness under identical challenges. In comparison with prior designs, RO-based PUF [21] exhibits extremely high stability but produces only a single fixed output, making the architecture less suitable for device authentication than strong PUF architectures. DDQ-APUF [17] applies a fault tolerance threshold that retains nearly all challenges but increases the risk of successful attacks during authentication, while discarding some challenges is generally acceptable because adding delay stages can increase the challenge space. In addition, the voltage range for the fault tolerance threshold is not specified, complicating assessment of stability and practicality under voltage variations. Genuine PUF [19] exhibits around 50% machine learning accuracy, but exposed responses in transmitted messages allow output response variations to be observed, enabling output-rule inference among genuine PUFs ($SPUF^G$ and $SPUF^F$); even with an exposed NVM key, the deception mechanism loses effectiveness, leading to vulnerability to replay and NVM attacks. NMQ PUF [22] uses two sets of ring oscillators for strong attack resistance but sacrifices reliability in a manner similar to XOR PUF, indicating that balance between resistance and reliability remains essential.

Table 11. Performance Comparison of PUF Architectures.

	[21] IEEE JSSC'20	[17] IEEE TCAS-I'25	[19] IEEE TCAD'21	[22] IEEE TVLSI'23	[23] IEEE TIFS'24	**Proposed Work**
Technology	28 nm	28 nm	28 nm	65 nm	28 nm	16 nm
PUF category	Weak	Strong	Strong	Strong	Strong	Strong
Type of PUF	Ring oscillator PUF	Arbiter PUF	Lightweight PUF	Ring oscillator PUF	Arbiter PUF	Arbiter PUF
High area overhead component	TDC	N/A	Large number of DFFs	N/A	TRNG	N/A
Experimental method	Chip	FPGA	FPGA	Chip	FPGA	Simulation
Reliability	99.992%	99.95%	93.9%	86.6%	98.3%	99.35% §
Uniformity	50.6%	50%	47%	50.5%	49.1%	50.18%

Table 11. *Cont.*

	[21] IEEE JSSC'20	[17] IEEE TCAS-I'25	[19] IEEE TCAD'21	[22] IEEE TVLSI'23	[23] IEEE TIFS'24	Proposed Work
Uniqueness/ Response diversity	49.94%	47.28%	40%	50%	49.8%	49.66% †
Machine Learning Prediction Accuracy	N/A	48% Training data: 2,000,000	50% Training data: 10,000	50% Training data: 2,000,000	58.71% Training data: 40,000,000	49.93% Training data: ~9200 ‡
Voltage range	0.4~1.3(V)	N/A	0.8~1.0(V)	N/A	N/A	0.675~1.05(V)
Temperature range	−40~125(°C)	−40~80 (°C)	0~70 (°C)	0~50 (°C)	−20~80(°C)	−40~150(°C)
Max. Operating Frequency	N/A	N/A	100 MHz	N/A	N/A	100 MHz
Power	[1] 0.275 mW @ 1 MHz	N/A	101 mW @ 100 MHz	0.237 mW	N/A	0.3089 mW @ 100 MHz 0.1541 mW @ 50 MHz

† For the proposed work, 49.66% denotes configuration-dependent response diversity obtained using different LFSR seeds and polynomials together with Monte Carlo process variations; the challenge sequence is not fixed across configurations, so this value does not represent conventional inter-device uniqueness. ‡ For the proposed-work ML entry, approximately 11,500 CRPs passed reliability screening; an 80/20 split provided approximately 9200 training-partition and 2300 testing CRPs, with a further 20% of the training portion reserved for MLP validation. § The proposed-work 99.35% reliability is the equal-weight mean of 20 selection-conditioned logarithmic scores from four three-PVT BST screening scenarios and five Monte Carlo models; the metrics and testing conditions are not directly matched across the cited designs. [1] For RO PUF [21], the power value is estimated by assuming a 1 MHz operating frequency to generate a 128-bit PUF response, resulting in a power consumption of 0.275 mW based on the reported energy value (2.15 pJ/bit).

Obfuscated-interconnection PUF [23] enhances resistance to machine learning attacks by increasing interconnection complexity in arbiter PUFs, but a True Random Number Generator (TRNG) and weak PUFs are introduced; the weak PUFs reduce reliability and the TRNG increases hardware cost, reducing suitability for resource-constrained IoT applications. Relative to architectures in [19,21,23] that rely on high-area-overhead components to improve PUF metric. The simulated SRPFD-PUF characteristics support its potential use in the illustrative authentication application, but an integrated device–server protocol was not implemented and no end-to-end authentication success rate was measured.

Although the proposed SRPFD-PUF has currently been evaluated through post-layout simulations, the design targets an ASIC-based silicon IP implementation for future IoT system integration. Compared with FPGA-based prototypes, an ASIC-based PUF IP offers the potential for on-chip integration with other digital and security modules, enabling compact and power-efficient SoC implementations. Future work will include tape-out and experimental chip characterization to validate the simulated performance and demonstrate the feasibility of the proposed architecture for practical IoT applications.

5.3. Protocol Performance

In (7), P represents the theoretical probability of obtaining at least Y correct outputs out of 100, assuming independent bit outcomes with a common per-bit correctness probability p. For Table 12, p denotes the assumed per-bit prediction accuracy; for Table 13, p denotes an illustrative per-bit matching probability based on the Hamming-distance reliability defined in (5), expressed as a fraction, rather than the logarithmic score in (3). These single-attempt model estimates are not measured whole-response error distributions or empirical false-acceptance/false-rejection rates, and do not cover repeated attempts or active protocol attacks.

$$P(X \geq Y) = \sum_{k=Y}^{100} \binom{100}{k} \cdot p^k \cdot (1-p)^{100-k} \tag{7}$$

Table 12. Theoretical Authentication Success Rates for 100-bit PUFs with Different Accuracy.

	$\frac{n_{tolerance}}{n}$	$\frac{6}{100}$	$\frac{8}{100}$	$\frac{10}{100}$	$\frac{12}{100}$
PUF Model Accuracy	0.55	4.21×10^{-18}	4.53×10^{-16}	2.91×10^{-14}	1.23×10^{-12}
	0.50	1.00×10^{-21}	1.60×10^{-19}	1.53×10^{-17}	9.56×10^{-16}

Table 13. Theoretical Authentication Success Probabilities for 100-bit PUFs with Different Assumed Per-Bit Matching Probabilities.

	$\frac{n_{tolerance}}{n}$	$\frac{7}{100}$	$\frac{8}{100}$	$\frac{9}{100}$	$\frac{10}{100}$
Reliability	0.96	0.9525	0.9810	0.9932	0.9978
	0.98	0.9991	0.9998	1.0000	1.0000
	0.99	1.0000	1.0000	1.0000	1.0000

In Tables 12 and 13, n denotes the total number of PUF response bits used for authentication, which is fixed at 100 bits in this study, while $n_{tolerance}$ represents the maximum number of bit errors allowed during authentication. Authentication is considered successful when the Hamming distance between the reference and received responses does not exceed $n_{tolerance}$, meaning that at least $n - n_{tolerance}$ bits must match. For example, when $n = 100$ and $n_{tolerance} = 8$, up to eight bit mismatches are permitted, requiring at least 92 correct response bits. The authentication success probability is evaluated using the binomial probability model in Equation (7), assuming independent and identically distributed bit outcomes. Table 12 reports the theoretical probability of satisfying the 100-bit response tolerance threshold under independent bit predictions with accuracies of 55% or 50%; it does not quantify active manipulation of protocol messages.

Table 13 presents authentication success probabilities under different reliability levels and tolerance bits, showing that authentication success remains close to 100% when the tolerance bit reaches 10 even when reliability is 96%. Therefore, machine learning prediction accuracy and circuit reliability are critical in selecting the number of tolerated error bits. The minimum selection-conditioned logarithmic reliability score in Table 9 is 98.93%, whereas the highest prediction accuracy among the evaluated machine-learning attacks in Table 10 is 52.46%; these distinct metrics do not directly determine the per-bit matching probability in Equation (7). For an illustrative 100-bit response with an eight-bit tolerance, Equation (7) gives a theoretical legitimate-device acceptance probability exceeding 99.999% when the assumed per-bit matching probability is 0.99, and a response-guessing probability of approximately 8.98×10^{-18} when the assumed attacker prediction accuracy is 0.5246.

To examine 100-bit response stability beyond the binomial approximation, archived post-layout SPICE data were reanalyzed using a job-wise offline enrollment procedure: for each of ten separately initialized LFSR simulation jobs and five Monte Carlo realizations, the first 100 positions passing the three-PVT BST screen were fixed against the nominal reference. At the two held-out conditions, (1.05 V, −40 °C) and (0.675 V, 150 °C), all 50 emulated 100-bit response records per condition satisfied the eight-error threshold (maximum conservative error counts of five and eight, respectively), counting unresolved output samples as errors. These results characterize simulation-based fixed-index response consistency, not measured legitimate-authentication acceptance or implemented NVM/firmware synchronization; the probabilities in Table 13 remain independent-bit theoretical estimates.

Table 14 compares the proposed protocol with recent PUF-based authentication protocols. For the proposed work, the TRNG comparison refers to a dedicated TRNG within the PUF hardware rather than to the platform-level entropy needed for X25519 and AES-CBC. In Table 14, PUF-independent indicates whether protocol operation depends on a specific PUF design, PUF software model needed indicates whether software modeling is required at the server for verification, TRNG needed indicates whether a true random number generator is required on the device side, Reverse engineering attack refers to resistance against reconstructing device-specific PUF responses from knowledge of the circuit architecture and publicly defined response-processing mechanisms alone under the respective threat models of the selected studies, Replay attack refers to the prevention of reuse of previously observed authentication records under each protocol's stated challenge-freshness rules, Hidden CRPs refers to preventing passive observation of network communication from revealing complete plaintext challenge–response pairs even when challenges are transmitted openly, and NVM attack for the proposed protocol concerns read-only disclosure of the server public key stored in device-side NVM, rather than public-key replacement or compromise of the server CRP database. These qualitative entries describe the protection mechanisms discussed in the selected studies and do not imply that all schemes have been experimentally evaluated under a common invasive-attack model. For the proposed illustrative exchange, the security-related entries in Table 14 represent intended mechanisms under the stated assumptions rather than experimentally verified end-to-end security properties. In particular, replay mitigation depends on server-enforced single-use challenges, AES-CBC provides no message-integrity authentication against active modification, and the reverse-engineering and NVM-related entries are restricted to the evaluated modeling attacks and read-only disclosure of the provisioned server public key. Except for the proposed protocol, the compared approaches require the server to build a software model of the PUF because emulation of challenge-response behavior is required for authentication.

Table 14. Performance Comparisons of The PUF Protocols.

	[19] IEEE TCAD'21	[20] IEEE TVLSI'22	[23] IEEE TIFS'24	[24] IEEE TCAS'25	Proposed Protocol
PUF-independent	√	×	×	×	√
PUF software model needed	√	√	√	√	×
TRNG needed	×	√	√	×	×
Reverse engineering attack	√	√	√	√	√
Replay attack	√	√	√	√	√
Hidden CRPs	×	√	×	√	√
NVM attack	×	No NVM	No NVM	No NVM	√

High generality is achieved because the proposed protocol is not designed for a specific type of PUF and is therefore applicable to various PUF architectures. Genuine CRPs are

registered without requiring additional software models to simulate PUF behavior, thereby simplifying system design. Compared to approaches such as [20,23] that require integration with a TRNG, computational and hardware resource overhead on IoT devices is reduced. The modeling-resistance results in Table 10 apply to the specified circuit-information disclosure and CRP-access assumptions, rather than establishing protection against invasive probing, firmware compromise, or unrestricted test-interface access. Moreover, AES-CBC conceals transmitted PUF responses, while single-use enrollment challenges limit replay of previously recorded responses without constituting general message-integrity protection.

In [19], a combination of real and fake PUFs hinders effective software modeling by attackers, and a deception mechanism disrupts data collection while fresh challenges prevent replay attacks; however, because CRPs are transmitted openly, vulnerability remains if keys are exposed and additional security measures are required. In [20], a dynamic response mechanism uses device-side TRNG to generate random indices and padding, ensuring unique and variable CRPs and enhancing resistance against reverse engineering. In [23], a Obfuscated-interconnection PUF with symmetrical obfuscation and challenge obfuscation uses a TRNG and weak PUF units to obfuscate challenges, and public transmission is made less exploitable. In [24], a 100% reliable software model is assumed, which is unrealistic because practical machine learning models incur prediction errors; therefore, tolerance to some erroneous bits is required to improve robustness.

The protocol limits replay of previously recorded responses by selecting a distinct enrolled challenge Ca for each authentication attempt and retiring it upon issuance. The 28-bit nonce N and session-dependent X25519 key derivation are retained for response encryption, but are not relied upon as substitutes for the single-use challenge rule or as guarantees of message integrity. The server's public key is stored in device-side NVM, and its disclosure alone does not reveal the session-specific shared secrets. However, compromise of the server's static private key could permit reconstruction of past shared secrets from recorded device ephemeral public keys.

A strong PUF is used as an example in the proposed protocol. If a more stable weak PUF as presented in [21] is adopted, a unique and stable output can be generated during enrollment and stored on the server for identity verification, and the same output can be reproduced during authentication for verification. Although some weak PUFs provide higher reliability than strong PUFs, fixed outputs create a single point of failure; once the enrolled key is compromised, device discard is required to maintain security. In contrast, a strong PUF supports multiple CRPs and provides redundancy, allowing challenge switching when a CRP is exposed without discarding the device. Lower reliability in strong PUFs can be mitigated by selecting stable CRPs (e.g., those consistent under varying voltage conditions) and applying error-tolerant mechanisms, allowing authentication success to approach 100%. Consequently, once a sufficient reliability level is achieved by the PUF circuit, perfect 100% reliability is not always necessary because extremely high reliability may increase circuit costs, while error-tolerant mechanisms in authentication can compensate for inherent reliability limitations. Under the independent-bit model in (7), the illustrative response-tolerance setting yields a theoretical legitimate-device acceptance probability exceeding 99.999%, not an observed end-to-end authentication success rate.

6. Conclusions

The SRPFD-PUF demonstrates near-ideal simulated uniformity, high reliability, configuration-dependent response diversity, and near-chance prediction accuracy under the evaluated machine-learning attacks. Overall PUF reliability is improved by reducing the dead zone in the sampling circuit. For a fair comparison, the original and proposed designs were evaluated under harsh environmental conditions, and the SRPFD-PUF is

shown to provide superior stability and robustness against environmental variations. An illustrative device–server authentication flow is also described, but authenticated messaging and end-to-end protocol security have not been implemented or validated; confidentiality of recorded encrypted responses in this example depends on the secrecy of the server's static private key. For a 100-bit response with an eight-bit tolerance, the independent-bit model in Equation (7) predicts a legitimate-device acceptance probability exceeding 99.999% at an assumed per-bit matching probability of 0.99 and a response-guessing probability on the order of 10^{-18} at an assumed attacker prediction accuracy of 0.5246; neither is a measured protocol outcome.

Author Contributions: Conceptualization, C.-C.C.; methodology, C.-C.C. and W.-C.H.; software, W.-C.H.; validation, C.-C.C. and W.-C.H.; writing—original draft preparation, C.-C.C., W.-C.H. and D.S.; writing—review and editing, C.-C.C. and D.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded in part by National Science and Technology Council of Taiwan under Grant NSTC-114-2221-E-194-060- and was financially/partially supported by the Advanced Institute of Manufacturing with High-tech Innovations (AIM-HI) from the Featured Areas Research Center Program within the framework of the Higher Education Sprout Project by the Ministry of Education (MOE) in Taiwan.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

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

Abbreviations

The following abbreviations are used in this manuscript:

AES	Advanced Encryption Standard
AES-CBC	Advanced Encryption Standard in Cipher Block Chaining Mode
AIM-HI	Advanced Institute of Manufacturing with High-tech Innovations
APUF	Arbiter Physically Unclonable Function
BST	Bit Self-Test
CBC	Cipher Block Chaining
CMA-ES	Covariance Matrix Adaptation Evolution Strategy
CRP	Challenge–Response Pair
DCT	Dynamic Challenge Transformation
DDQ-APUF	Delay Difference Quantization Arbiter PUF
DFF	D-Type Flip-Flop
DRAM	Dynamic Random-Access Memory
FinFET	Fin Field-Effect Transistor
FPGA	Field-Programmable Gate Array
HD	Hamming Distance
HKDF	HMAC-Based Extract-and-Expand Key Derivation Function
HMAC	Hash-Based Message Authentication Code
HW	Hamming Weight
IoT	Internet of Things
LFSR	Linear Feedback Shift Register
ML	Machine Learning
NMQ	Nonmonotonic Response Quantization
PFD	Phase-Frequency Detector
PUF	Physically Unclonable Function
SRPFD	SR-Latch-Based Phase-Frequency Detector
SRPFD-PUF	SR-Latch-Based Phase-Frequency Detector PUF
SVM	Support Vector Machine
TRNG	True Random Number Generator

References

1. Diedhiou, O.N.; Diallo, C. An IoT mutual authentication scheme based on PUF and blockchain. In Proceedings of the IEEE International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 16–18 December 2020; pp. 1034–1040.
2. Kim, B.; Yoon, S.; Kang, Y. PUF-based IoT device authentication scheme on IoT open platform. In Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Republic of Korea, 20–22 October 2021; pp. 1873–1875.
3. Rincón, A.E.R.; Melo, W.S., Jr.; Farias, C.M.; Carmo, L.F.R.C. Securing smart meters through physical properties of their components. *IEEE Trans. Instrum. Meas.* **2020**, *70*, 3000511. [CrossRef]
4. Ruhrmair, U.; Holcomb, D.E. PUFs at a glance. In Proceedings of the Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, Germany, 24–28 March 2014; pp. 1–6.
5. Herder, C.; Yu, M.D.; Koushanfar, F.; Devadas, S. Physical unclonable functions and applications: A tutorial. *Proc. IEEE* **2014**, *102*, 1126–1141. [CrossRef]
6. Fruhashi, K.; Shiozaki, M.; Fukushima, A.; Murayama, T.; Fujino, T. The arbiter-PUF with high uniqueness utilizing novel arbiter circuit with delay-time measurement. In Proceedings of the IEEE International Symposium of Circuits and Systems (ISCAS), Rio de Janeiro, Brazil, 15–18 May 2011; pp. 2325–2328.
7. Yoon, S.; Kim, B.; Kang, Y. Multiple PUF-based lightweight authentication method in the IoT. In Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Republic of Korea, 20–22 October 2021; pp. 1198–1200.
8. Hori, Y.; Yoshida, T.; Katashita, T.; Satoh, A. Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs. In Proceedings of the International Conference on Reconfigurable Computing and FPGAs, Cancun, Mexico, 13–16 December 2010; pp. 298–303.
9. 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 Des. Integr. Circuits Syst.* **2022**, *41*, 4433–4444. [CrossRef]
10. Rukhin, A.; Soto, J.; Nechvatal, J.; Smid, M.; Barker, E. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*; 800-22 Rev. 1a; NIST Special Publication: Gaithersburg, MD, USA, 2010.
11. Zhang, J.; Tan, X.; Zhang, Y.; Wang, W.; Qin, Z. Frequency offset-based ring oscillator physical unclonable function. *IEEE Trans. Multi-Scale Comput. Syst.* **2018**, *4*, 711–721. [CrossRef]
12. Li, J.; Gao, H.; Cui, Y.; Wang, C.; Wang, Y.; Gu, C.; Liu, W. Theoretical analysis of configurable RO PUFs and strategies to enhance security. In Proceedings of the IEEE International Workshop on Signal Processing Systems (SiPS), Nanjing, China, 20–23 October 2019; pp. 91–96.
13. Amsaad, F.; Razaque, A.; Baza, M.; Kose, S.; Bhatia, S.; Srivastava, G. An efficient and reliable lightweight PUF for IoT-based applications. In Proceedings of the IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada, 14–18 June 2021; pp. 1–6.
14. Avvaru, S.V.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]
15. Suh, G.E.; Devadas, S. Physical unclonable functions for device authentication and secret key generation. In Proceedings of the 44th ACM/IEEE Design Automation Conference (DAC), San Diego, CA, USA, 4–8 June 2007; pp. 9–14.
16. He, Z.; Chen, W.; Zhang, L.; Chi, G.; Gao, Q.; Harn, L. A highly reliable arbiter PUF with improved uniqueness in FPGA implementation using bit-self-test. *IEEE Access* **2020**, *8*, 181751–181762. [CrossRef]
17. Wang, Y.; Zhang, G.; Mei, X.; Gu, C. A high-reliability, non-CRP-discard arbiter PUF based on delay difference quantization. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2025**, *72*, 573–585. [CrossRef]
18. Zhang, J.; Shen, C. Set-based obfuscation for strong PUFs against machine learning attacks. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2021**, *68*, 288–300. [CrossRef]
19. Gu, C.; Chang, C.H.; Liu, W.; Yu, S.; Wang, Y.; O'Neill, M. A modeling attack resistant deception technique for securing lightweight-PUF-based authentication. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **2021**, *40*, 1183–1196. [CrossRef]
20. Wang, Y.; Wang, C.; Gu, C.; Cui, Y.; O'Neil, 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]
21. Liang, Z.Y.; Wei, H.H.; Liu, T.T. A wide-range variation resilient physically unclonable function in 28 nm. *IEEE J. Solid-State Circuits* **2020**, *55*, 817–825. [CrossRef]
22. Stangherlin, K.; Wu, Z.; Patel, H.; Sachdev, M. Enhancing strong PUF security with nonmonotonic response quantization. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2023**, *31*, 55–64. [CrossRef]

23. 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]
24. Mexis, N.; Anagnostopoulos, N.A.; Katzenbeisser, S.; Kavun, E.B.; Tehranipoor, S.; Arul, T. Achieving error-free lightweight authentication with DRAM-based physical unclonable functions. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2025**, *72*, 637–646. [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.