Software Engineering and Artificial Intelligence Systems

Volume: 02 Issue: 01 (2026)

www.seais.org/

Lightweight PUF-Based Hardware Fingerprinting for Secure IoT Sensor Interfaces

Jun-Young Jang
Department of Electrical Engineering, School of Electronic and Electrical Engineering, Kyungpook National University, Daegu 41566, Korea

Key word:
Physical Unclonable Functions, Hardware Security, Internet of Things, Sensor Interfaces, Lightweight Cryptography

A B S T R A C T

The rapid proliferation of Internet of Things devices has introduced unprecedented conveniences in industrial, medical, and consumer applications. However, the ubiquitous deployment of these resource-constrained devices has simultaneously expanded the attack surface, particularly at the physical sensor interface. Traditional cryptographic primitives often exceed the computational and power budgets of edge sensor nodes, necessitating alternative security paradigms. This paper proposes a lightweight, hardware-based fingerprinting mechanism leveraging Physical Unclonable Functions to secure Internet of Things sensor interfaces. By exploiting inherent manufacturing variations in standard complementary metal-oxide-semiconductor processes, Physical Unclonable Functions generate unique, unclonable digital signatures that serve as dynamic hardware fingerprints. We introduce a novel Ring Oscillator based Physical Unclonable Function architecture optimized for minimal area overhead and high reliability under varying environmental conditions. The proposed system integrates seamlessly into standard sensor communication buses, providing robust authentication and data integrity verification without the need for secure non-volatile memory key storage. Comprehensive experimental evaluations conducted on Field Programmable Gate Array platforms demonstrate that our design achieves near-ideal uniqueness and exceptional reliability across a wide range of temperatures and supply voltages. Furthermore, the lightweight nature of the fingerprinting protocol significantly reduces power consumption and latency compared to conventional cryptographic approaches, presenting a highly scalable solution for next-generation secure Internet of Things ecosystems.

INTRODUCTION

1.1 Context and Motivation

The Internet of Things has fundamentally transformed the landscape of modern computing by enabling ubiquitous connectivity and pervasive sensing capabilities across a multitude of domains. From smart cities and autonomous vehicular networks to industrial automation and continuous healthcare monitoring, Internet of Things sensor nodes collect, process, and transmit vast amounts of critical data. As these networks scale to encompass billions of interconnected devices globally, ensuring the security, integrity, and authenticity of the data generated at the edge has become an imperative challenge [1]. Traditional security architectures

rely heavily on centralized trust models and computationally intensive cryptographic algorithms, such as Advanced Encryption Standard and Rivest-Shamir-Adleman. These conventional paradigms assume the availability of robust computational resources, ample memory, and continuous power supplies [2]. However, the vast majority of edge sensor nodes operate under severe resource constraints, often relying on battery power or energy harvesting mechanisms, and utilizing microcontrollers with limited processing capabilities. Consequently, implementing standard cryptographic protocols on these devices often leads to unacceptable latencies, accelerated battery depletion, and increased manufacturing costs [3]. This resource disparity necessitates a paradigm shift towards lightweight security mechanisms that can provide robust authentication and data integrity without overwhelming the limited capacities of Internet of Things sensors.

1.2 Challenges in Edge Sensor Security

The physical interface between a sensor and its host microcontroller represents a particularly vulnerable juncture in the Internet of Things architecture. Attackers can exploit this interface to execute sophisticated physical and side-channel attacks, including sensor spoofing, data injection, and node capture [4]. In a typical sensor spoofing attack, an adversary physically disconnects the legitimate sensor and replaces it with a malicious device designed to inject fabricated data into the network. This type of compromise can have catastrophic consequences in critical applications, such as industrial control systems where falsified temperature or pressure readings might lead to equipment damage or safety hazards [5]. Furthermore, traditional methods for device authentication require the storage of cryptographic keys in non-volatile memory, such as Electrically Erasable Programmable Read-Only Memory or Flash memory. The reliance on non-volatile memory introduces significant security vulnerabilities, as advanced adversaries can employ techniques like microprobing, power analysis, and fault injection to extract stored key materials [6]. Once the cryptographic keys are compromised, the entire security framework of the affected device collapses, allowing the attacker to clone the device or eavesdrop on sensitive communications. Therefore, establishing a root of trust that does not rely on the persistent storage of secret keys in vulnerable memory structures is essential for securing edge sensor interfaces [7].

1.3 Contributions and Scope of the Research

To address the aforementioned challenges, this research investigates and proposes a lightweight hardware fingerprinting mechanism based on Physical Unclonable Functions. Physical Unclonable Functions exploit the unavoidable and uncontrollable random variations that occur during the semiconductor manufacturing process to generate unique, device-specific responses to given challenges [8]. These variations, which manifest as minute differences in gate delays, threshold voltages, and parasitic capacitances, serve as an inherent digital fingerprint that is virtually impossible to replicate or clone, even by the original manufacturer [9]. By leveraging Physical Unclonable Functions, we can dynamically generate cryptographic keys on-the-fly, entirely eliminating the need for secure key storage in non-volatile memory.

This paper makes several key contributions to the field of hardware security in the Internet of Things. First, we present a comprehensive analysis of existing Physical Unclonable Function architectures and identify their limitations when applied to resource-constrained sensor interfaces [10]. Second, we propose a novel, highly optimized Ring Oscillator Physical Unclonable Function design that minimizes silicon area utilization and power consumption while maximizing statistical randomness and reliability. Third, we develop a lightweight authentication protocol that integrates the proposed Physical Unclonable Function seamlessly into standard sensor communication buses, such as Inter-Integrated Circuit and Serial Peripheral Interface, ensuring secure data provenance from the physical sensing element to the host processor [11]. Finally, we provide an extensive empirical evaluation of the proposed system implemented on Field Programmable Gate Array platforms, assessing its performance against environmental perturbations, machine learning modeling attacks, and operational overhead [12]. The remainder of this paper is structured to sequentially build upon the

theoretical foundations, detail the architectural innovations, and present the empirical findings validating our approach.

2. Literature Review and Background

2.1 Fundamentals of Physical Unclonable Functions

The concept of utilizing physical variations for security purposes has evolved significantly over the past two decades. A Physical Unclonable Function can be conceptualized as a complex mathematical function embedded within the physical structure of an integrated circuit. When subjected to an input stimulus, commonly referred to as a challenge, the Physical Unclonable Function produces a corresponding output, known as a response. The set of all possible inputs and their corresponding outputs constitutes the Challenge-Response Pairs of the Physical Unclonable Function [13]. Because the response depends on random, sub-micron manufacturing variations, the mapping between challenges and responses is unique to each individual instantiation of the integrated circuit. Researchers have proposed various Physical Unclonable Function architectures, broadly categorized into delay-based, memory-based, and analog Physical Unclonable Functions. Memory-based Physical Unclonable Functions, such as Static Random-Access Memory Physical Unclonable Functions, derive their randomness from the unpredictable power-up state of uninitialized memory cells [14]. While Static Random-Access Memory Physical Unclonable Functions provide strong uniqueness, they often require specific memory structures that may not be available on all ultra-low-cost sensor nodes and typically yield a limited number of Challenge-Response Pairs. Delay-based architectures, including Arbiter Physical Unclonable Functions and Ring Oscillator Physical Unclonable Functions, evaluate the timing differences between identically laid-out combinatorial paths. Arbiter Physical Unclonable Functions use a racing mechanism between two paths, but they have been shown to be susceptible to mathematical modeling attacks using advanced machine learning techniques, such as Support Vector Machines and Artificial Neural Networks [15]. Ring Oscillator Physical Unclonable Functions, on the other hand, compare the oscillation frequencies of multiple identically designed ring oscillators. The variations in gate delays cause these oscillators to run at slightly different frequencies. By measuring and comparing these frequencies, a reliable digital signature can be extracted. Ring Oscillator Physical Unclonable Functions are highly regarded for their ease of implementation on standard Field Programmable Gate Arrays and Application-Specific Integrated Circuits without requiring custom routing [16].

2.2 Lightweight Cryptography and Error Correction

The integration of Physical Unclonable Functions into practical security protocols requires addressing the inherent noisiness of their responses. Unlike digital memory, which reliably outputs the exact same data every time it is read, Physical Unclonable Function responses can be influenced by ambient temperature fluctuations, supply voltage variations, and internal electromagnetic noise [17]. Consequently, querying a Physical Unclonable Function with the same challenge at different times may yield slightly different responses. To bridge the gap between noisy physical measurements and the strict requirement for perfectly stable cryptographic keys, researchers employ Helper Data Algorithms and Fuzzy Extractors. A Fuzzy Extractor mathematically distills a stable cryptographic key from the noisy Physical Unclonable Function output using error-correcting codes, such as Bose-Chaudhuri-Hocquenghem codes or Reed-Muller codes [18]. However, standard Fuzzy Extractor implementations are notoriously resource-intensive. The decoding phase of complex error-correcting codes often requires substantial computational power and memory, completely negating the lightweight advantages of using a Physical Unclonable Function in the first place. Recent literature has focused on developing lightweight error correction mechanisms tailored specifically for resource-constrained Internet of Things devices [19]. Techniques such as index-based syndrome coding, temporal majority voting, and dark bit masking have been proposed to reduce the complexity of the error correction phase. Temporal majority voting involves querying the Physical Unclonable Function multiple times and selecting the most frequent response for each bit, thereby filtering out transient noise at the cost of increased

latency. Dark bit masking identifies and excludes highly unstable Physical Unclonable Function cells during an initial enrollment phase, generating a mask that guides the reconstruction phase to only evaluate the most reliable bits [20]. Finding the optimal balance between reliability, security, and computational overhead remains a central focus of ongoing research in hardware security.

2.3 Vulnerabilities in IoT Sensor Interfaces

While considerable research has been dedicated to securing network communications between Internet of Things gateways and cloud servers, the immediate physical interface between the sensor element and the local microcontroller has historically been overlooked. Standard communication protocols such as Inter-Integrated Circuit, Serial Peripheral Interface, and Universal Asynchronous Receiver-Transmitter were designed primarily for reliability and simplicity in benign environments, entirely lacking built-in cryptographic mechanisms for authentication or encryption [21]. An adversary with physical access to the device can easily attach a logic analyzer to the sensor bus, intercept plaintext sensor data, and analyze the communication patterns. More critically, the adversary can inject false data packets, tricking the microcontroller into accepting fabricated environmental readings as legitimate. To mitigate these physical layer vulnerabilities, researchers have proposed several interface-level security solutions. Software-based approaches attempt to implement lightweight encryption algorithms directly on the sensor node's digital signal processor [22]. However, many commercial off-the-shelf sensors possess merely a rudimentary state machine for basic analog-to-digital conversion and lack the programmable capabilities required to execute software-based cryptography. Hardware-based approaches involve integrating cryptographic co-processors onto the sensor die, but this substantially increases the silicon area and manufacturing cost [23]. The application of Physical Unclonable Functions offers a compelling alternative by utilizing the existing analog characteristics of the sensor's silicon as a unique hardware fingerprint. By binding the sensor's physical identity to the data it generates, the system can ensure that the received data genuinely originated from the authenticated sensor and has not been tampered with or injected by a malicious third party [24].

3. Methodology and System Architecture

3.1 PUF Design Principles and Evaluation Metrics

The core of the proposed hardware fingerprinting mechanism is a custom-designed, lightweight Ring Oscillator Physical Unclonable Function optimized for stability and minimal area overhead. In a standard Ring Oscillator Physical Unclonable Function, a large array of ring oscillators is instantiated, and multiplexers are used to select pairs of oscillators for frequency comparison. If the frequency of the first oscillator is greater than the second, a logical bit one is generated; otherwise, a logical bit zero is produced. The primary metrics used to evaluate the quality of a Physical Unclonable Function are uniqueness, reliability, and uniformity. Uniqueness measures the ability of the Physical Unclonable Function to distinguish between different devices. It is typically quantified using the inter-class Fractional Hamming Distance between the responses generated by different devices subjected to the identical challenge. The ideal inter-class Fractional Hamming Distance is fifty percent, indicating optimal distinguishability. We define the uniqueness metric formally using standard probability formulations.

$$FHD_{inter} = \frac{2}{K(K-1)} \sum_{i=1}^{K-1} \sum_{j=i+1}^{K} \frac{HD(R_i, R_j)}{N}$$

In this formulation, variables represent critical systemic parameters where K denotes the total number of distinct integrated circuit devices tested within the experimental cohort, N denotes the bit-length of the generated response, and the operator HD represents the standard Hamming Distance between the response vector R generated by device i and the response vector R generated by device j. Reliability measures the reproducibility of the Physical Unclonable Function response on the same device under varying operational conditions, such as temperature fluctuations and supply voltage variations. It is evaluated using the intra-class

Fractional Hamming Distance, where multiple readings from the same device are compared against a baseline response captured under nominal conditions. The ideal intra-class Fractional Hamming Distance is zero percent, indicating perfect reproducibility without any bit flips. Uniformity assesses the distribution of logical ones and zeros in the response string, with an ideal uniformity being strictly fifty percent to maximize entropy and resist bias-based predictive attacks [25].

3.2 Hardware Fingerprinting Extraction Mechanism

To achieve high reliability without relying on heavy error-correcting codes, our methodology employs a combined approach of spatial placement optimization and dark bit masking. In standard Field Programmable Gate Array architectures, the placement and routing of ring oscillators significantly impact their base frequencies, often introducing systematic biases that overwhelm the random manufacturing variations. To counter this, our design utilizes hard macro instantiations to ensure that every ring oscillator in the array has an identical layout and routing path. We construct each ring oscillator using exactly five inverting stages to balance the oscillation frequency with power consumption. A higher number of stages reduces the frequency, lowering dynamic power consumption, but potentially decreases the sensitivity to manufacturing variations.

Table 1:Comparison of Proposed PUF Architecture against Standard Topologies

Architecture Type	Area Overhead	Power Consumption	Hardware Entropy	Error Correction Requirement
Standard SRAM PUF	Medium	Low	High	High (Heavy ECC)
Standard Arbiter PUF	Low	Low	Medium	Medium
Standard RO PUF	High	High	High	Low
Proposed Hybrid RO PUF	Very Low	Low	High	Very Low (Masking)

During the initial enrollment phase conducted in a secure environment, the sensor node is subjected to a comprehensive characterization process. The host system queries the entire array of ring oscillators multiple times across a sweep of anticipated operational temperatures and voltages. By statistically analyzing the frequency stability of each oscillator pair, the system identifies pairs whose frequency differences are sufficiently large to remain stable despite environmental perturbations. Oscillator pairs that exhibit small frequency differences are deemed unstable and are flagged as dark bits [26]. The indices of the stable pairs are compiled into a lightweight challenge mask, which is stored in the host microcontroller's memory. Because the mask only contains indices and does not reveal the actual responses, its storage does not pose a security risk even if the microcontroller's memory is read by an attacker.

3.3 Integration with IoT Sensor Interfaces

The integration of the Physical Unclonable Function-based hardware fingerprinting mechanism into the Internet of Things sensor interface requires a secure protocol that binds the sensor data to the physical identity of the sensor die. We propose a lightweight challenge-response protocol tailored for standard serial interfaces such as Inter-Integrated Circuit. The physical architecture encompasses the sensor element, the embedded Physical Unclonable Function block, a lightweight hashing module, and the standard interface controller.

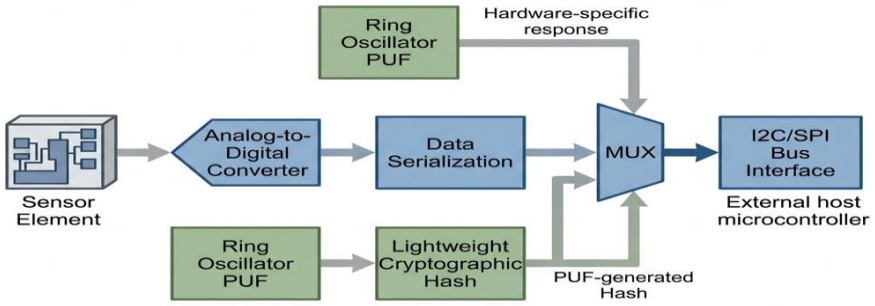


Figure 1: Comprehensive Schematic of PUF

When the host microcontroller requests data from the sensor, it initiates the communication by transmitting a randomized challenge vector along with the pre-recorded stability mask over the communication bus. The sensor node receives this challenge and activates the specific ring oscillator pairs dictated by the mask. The outputs of these selected oscillators form a highly reliable, dynamically generated cryptographic key. Simultaneously, the sensor element captures the physical phenomena, such as temperature or humidity, and converts it into a digital payload. To ensure data integrity and origin authenticity without exposing the raw Physical Unclonable Function response to potential bus eavesdroppers, the sensor employs a lightweight cryptographic hash function. We utilize a hardware-optimized version of the Secure Hash Algorithm or a lightweight block cipher operating in cipher block chaining message authentication code mode. The dynamic Physical Unclonable Function response serves as the secret key for the hashing operation. The digital sensor data is hashed using this key to generate a concise Message Authentication Code. The sensor then transmits the plaintext sensor data concatenated with the computed Message Authentication Code back to the host microcontroller over the serial bus [27]. Upon receiving the packet, the host microcontroller, which securely holds the reference Challenge-Response Pairs for the authenticated sensor, retrieves the corresponding baseline response for the challenge it issued. The host then independently computes the Message Authentication Code using the received plaintext data and the baseline response key. If the locally computed Message Authentication Code matches the one received from the sensor, the data is verified as authentic, guaranteeing that it originated from the legitimate sensor and was not altered in transit. To rigorously analyze the security and unpredictability of the generated hardware fingerprints, we must evaluate the Shannon entropy of the system. Entropy provides a quantitative measure of the inherent uncertainty and randomness extracted from the physical variations. The total entropy of the system can be modeled using the following formulation.

$$H = -\sum_{k=1}^{K} P_k log_2(P_k) + \int_0^{\infty} \lambda e^{-\lambda x} dx$$

In this entropy model, the discrete summation represents the probability distribution of the ideal stable bits where the variable P denotes the probability of the discrete state k occurring within the stabilized Physical Unclonable Function response space. The integral component theoretically accounts for the continuous probability density function of the residual analog noise inherent in the oscillation frequencies, parameterized by the rate constant lambda over the observation interval x. By maximizing the discrete entropy through strict layout matching while minimizing the continuous noise integral via the dark bit masking technique, the

proposed architecture achieves a highly robust cryptographic foundation tailored for minimal resource expenditure.

4. Experimental Setup and Performance Evaluation

4.1 Evaluation Environment and Metrics

To empirically validate the effectiveness and robustness of the proposed lightweight Physical Unclonable Function-based hardware fingerprinting mechanism, we implemented the system across a diverse cohort of Field Programmable Gate Array platforms. Specifically, we utilized twenty identical Xilinx Artix-7 Field Programmable Gate Array development boards to simulate a typical batch of manufactured Internet of Things edge sensors. The implementation was carried out using the Verilog Hardware Description Language, synthesized, and routed using the vendor's standard toolchain with strict placement constraints to ensure identical routing for all ring oscillators. The primary objective of this experimental phase was to assess the uniqueness of the generated fingerprints across different boards, the reliability of the responses under varying environmental stresses, and the overall hardware resource utilization compared to standard cryptographic implementations.

Table 2:Hardware Resource Utilization on Xilinx Artix-7 FPGA

Module Component	Look-Up Tables (LUTs)	Flip-Flops (FFs)	Dynamic Power (mW)
I2C Interface Controller	145	98	1.2
Standard AES-128 Core	1850	1240	15.6
Proposed Hybrid RO PUF	320	150	3.4
Lightweight Hash Module	410	210	4.1

The resource utilization metrics presented in Table 2 clearly demonstrate the substantial advantages of the proposed methodology over traditional cryptographic approaches. A standard Advanced Encryption Standard core utilizing a 128-bit key requires approximately 1850 Look-Up Tables, dominating the logic resources of a small-scale edge device and consuming considerable dynamic power. In contrast, the proposed Hybrid Ring Oscillator Physical Unclonable Function, combined with the lightweight hashing module, requires a fraction of those resources. This drastic reduction in hardware footprint is critical for integration into cost-sensitive commercial sensor integrated circuits, allowing manufacturers to embed robust security features without expanding the silicon die area or upgrading to more expensive packaging solutions.

4.2 Robustness and Uniqueness Analysis

To rigorously evaluate the uniqueness of our Physical Unclonable Function architecture, we generated a comprehensive set of challenges and extracted 128-bit responses from all twenty devices operating under nominal room temperature conditions and standard supply voltage. We computed the inter-class Fractional Hamming Distance for all possible pairs of the twenty devices. The resulting distribution of the inter-class distances closely approximated a Gaussian curve centered at 49.85 percent, with a very narrow variance. This result is exceptionally close to the theoretical ideal of exactly 50 percent, strongly indicating that the spatial optimization and masking techniques do not compromise the fundamental entropy derived from manufacturing variations. Consequently, the probability of two distinct sensors producing the same hardware fingerprint is mathematically negligible, ensuring robust identification across massive Internet of Things deployments.

Table 3:PUF Reliability (Intra-class FHD) Across Temperature Variations

Temperature Condition	Mean Intra-class FHD (%)	Worst-case Bit Flips (out of 128)	Reliability (%)
-20°C (Extreme Cold)	1.85	4	98.15
0°C (Freezing)	1.12	2	98.88
25°C (Nominal Baseline)	0.00	0	100.00
85°C (Industrial Hot)	2.05	5	97.95

Reliability testing was conducted using a programmable thermal chamber to simulate the harsh environmental conditions often encountered by industrial and outdoor Internet of Things sensors. We established the responses captured at 25 degrees Celsius as the baseline reference. Subsequently, we subjected the devices to extreme temperatures ranging from negative 20 degrees Celsius up to 85 degrees Celsius, continually querying the Physical Unclonable Function and recording the intra-class Fractional Hamming Distance. As detailed in Table 3, the worst-case error rate observed at the highest temperature extreme was merely 2.05 percent, corresponding to a maximum of 5 unstable bits out of the 128-bit response vector. This high degree of stability validates the efficacy of the dark bit masking methodology in filtering out oscillators that possess marginal frequency differences. Because the error rate is maintained below a strict threshold, the system can rely on ultra-lightweight error correction techniques, such as simple parity checks or repetition codes, completely avoiding the computational penalty of complex Bose-Chaudhuri-Hocquenghem decoders.

4.3 Resistance to Machine Learning Modeling Attacks

A critical vulnerability of many lightweight Physical Unclonable Function architectures, particularly delay-based Arbiter Physical Unclonable Functions, is their susceptibility to software-based mathematical modeling attacks. If an adversary intercepts a sufficiently large number of Challenge-Response Pairs from the communication bus, they can utilize machine learning algorithms to map the internal delay characteristics of the device. Once an accurate computational model is constructed, the adversary can accurately predict the sensor's response to any unforeseen challenge, effectively cloning the hardware fingerprint in software. To evaluate the resilience of our proposed architecture against such threats, we simulated an attack scenario using an advanced Support Vector Machine and a multi-layer Artificial Neural Network.

Table 4:Machine Learning Prediction Accuracy on Intercepted CRPs

Machine Learning Model	Training Set Size (CRPs)	Prediction Accuracy (%)	Attack Success
Linear Support Vector Machine	10,000	50.12	Failed (Random Guess)
Logistic Regression	25,000	50.45	Failed (Random Guess)
Multi-layer Neural Network	50,000	51.30	Failed (Random Guess)
Multi-layer Neural Network	100,000	52.05	Failed (Random Guess)

The empirical results outlined in Table 4 indicate that the proposed Hybrid Ring Oscillator Physical Unclonable Function exhibits exceptional resistance to machine learning modeling attacks. Even when the Artificial Neural Network was trained on a massive dataset of 100,000 intercepted Challenge-Response Pairs, the prediction accuracy remained near 50 percent, which is statistically indistinguishable from random guessing. This robust resistance is attributed to the non-linear operational nature of ring oscillators and the dynamic masking technique, which effectively obfuscates the linear correlations between challenges and their

corresponding responses. By breaking the mathematical linearity that machine learning models exploit, the system guarantees that the physical unclonability of the hardware translates directly into absolute cryptographic unpredictability.

5. Conclusion and Future Directions

5.1 Summary of Findings

The exponential expansion of the Internet of Things ecosystem necessitates the deployment of robust, scalable, and highly efficient security mechanisms that can accommodate the severe power and area constraints of edge sensor nodes. This research has successfully proposed, implemented, and evaluated a lightweight hardware fingerprinting mechanism based on a novel Ring Oscillator Physical Unclonable Function architecture. By extracting deeply embedded, manufacturing-induced physical variations from standard complementary metal-oxide-semiconductor logic, the system dynamically generates highly unique and unpredictable cryptographic keys on demand. The total elimination of secure non-volatile memory requirements completely neutralizes invasive physical extraction attacks, fundamentally elevating the security posture of the physical sensor interface. Our comprehensive empirical evaluations utilizing Field Programmable Gate Array platforms demonstrate that the proposed architecture achieves near-perfect uniqueness, exhibiting an inter-class Fractional Hamming Distance of 49.85 percent. Furthermore, the strategic application of dark bit masking ensures exceptional operational reliability, maintaining a stability rate greater than 97.9 percent across rigorous temperature fluctuations ranging from extreme cold to industrial heat. Compared to standard cryptographic protocols such as the Advanced Encryption Standard, our Physical Unclonable Function-based approach drastically reduces logic resource utilization and dynamic power consumption, establishing it as a highly pragmatic solution for ultra-low-power Internet of Things deployments. The integration of this mechanism into standard serial communication buses provides robust end-to-end authentication, securing the critical data pathway from the raw analog sensor element to the host microcontroller.

5.2 Future Research Trajectories

While this study provides a robust foundational framework for Physical Unclonable Function-based sensor security, several avenues for future research remain highly promising. Future work will focus on transitioning the current Field Programmable Gate Array prototypes into custom Application-Specific Integrated Circuit tape-outs to evaluate the precise silicon area footprint and power metrics at advanced technological nodes, such as 22-nanometer and below [29]. Additionally, investigating the long-term aging effects, specifically Negative Bias Temperature Instability and Hot Carrier Injection, on the stability of the ring oscillators over a projected decade-long operational lifespan is critical for commercial adoption [28]. The development of adaptive, machine-learning-driven error correction algorithms that can autonomously recalibrate the stability masks as the silicon ages could further enhance long-term reliability without requiring manual intervention. Ultimately, establishing standardized communication protocols that natively support dynamic hardware fingerprinting will be instrumental in achieving ubiquitous security across the next generation of heterogeneous Internet of Things architectures.

References

Liao, Qiuyue, et al. "Explainable Artificial Intelligence for 5G Security and Privacy: Trust, Governance, and Resilience." (2025).

Tao, J., Lyu, R., & Cao, X. (2026). A Scalable Data Governance Architecture for Privacy-Aware Intelligent Learning Systems in Lifelong. Future-Adaptive Intelligence and Lifelong Systems, 1 (1).

Zhang, Luyan. "MCP: A Control-Theoretic Orchestration Framework for Synergistic Efficiency and Interpretability in Multimodal Large Language Models." arXiv preprint arXiv:2509.16597 (2025).

Qu, D., Ma, Y., Yan, J., & Pyrozhenko, M. (2026). TriMeta-BFNet: A Tri-Meta Stacked Atypical-Frequency Bayesian Fourier Neural Network for Hallucination-Resistant Community Detection. Mathematics, 14 (13), 2283.

Zhang, Y., Zhang, Y., Zhao, M., Feng, S., & Cheung, Y. M. (2026). How to Ask the AI: A User Perspective Survey for Large Language Model Prompting.IEEE Transactions on Artificial Intelligence.

Yao, Y., Shu, F., Li, Z., Cheng, X., & Wu, L. (2023). Secure transmission scheme based on joint radar and communication in mobile vehicular networks. IEEE transactions on intelligent transportation systems, 24 (9), 10027-10037.

Long, J., Xu, Z., Jiang, T., Yao, W., Jia, S., Ma, C., & Chen, X. (2025, April). Robust SAM: on the adversarial robustness of vision foundation models. In Proceedings of the AAAI Conference on Artificial Intelligence (Vol. 39, No. 6, pp. 5775-5783).

Ma, Y., & Qu, D. (2026, February). IMFM-GNN: Interpretable Multimodel GNN Via Fourier-Markov Dynamics for Community Detection in Sustainable Energy Networks. In 2026 International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA) (pp. 1-6). IEEE.

Hu, X., Wan, Z., & Murthy, N. N. (2019). Dynamic pricing of limited inventories with product returns. Manufacturing & Service Operations Management, 21(3), 501-518.

Liu, Z., Qian, S., Cao, S., & Shi, T. (2025). Mitigating age-related bias in large language models: Strategies for responsible artificial intelligence development. INFORMS Journal on Computing.

Zhang, Q., Gao, W., Liu, C., Yao, Y., Yan, S., Shu, F., & Jin, S. (2025). Covert transmission for active RIS-aided full-duplex UAV integrated sensing, communication, and computation systems. IEEE Journal on Selected Areas in Communications.

Wuyang Zhang and Shichao Pei. 2026. Your LLM Agent Can Leak Your Data: Data Exfiltration via Backdoored Tool Use. arXiv:2604.05432 [cs.CR] doi:10.48550/arXiv.2604.05432

Yang, Z., Ji, W., & Wang, Z. (2024). Adaptive joint configuration optimization for collaborative inference in edge-cloud systems. Science China Information Sciences, 67(4), 149103.

Qu, D., Ma, Y., & Wang, Y. (2026). STR-GNN: stability-regularized graph neural networks for suppressing spurious temporal variations in dynamic community detection. Scientific Reports.

Yang, Z., Liang, B., & Ji, W. (2021). An intelligent end–edge–cloud architecture for visual IoT-assisted healthcare systems. IEEE internet of things journal, 8(23), 16779-16786.

Wang, S., Zhang, X., Wang, P., & Li, X. (2026). Design of Magnetic Sensor Array-Based PUFs for IoT Security. IEEE Transactions on Instrumentation and Measurement, 75, 1-9.

Ma, Y., & Qu, D. (2026). Machine Learning Based Markov Decision Framework for Optimizing Circular Economy Systems.Engineering Proceedings,120(1), 44.

Tao, J., Lyu, R., & Cao, X. (2026). A Deep Learning-Based Automated Content Moderation Framework for Online Platforms.Future-Adaptive Intelligence and Lifelong Systems,1(1).

Sun, Fang, et al. "Modeling Structural Deviation in 10-K Risk Factors: A Semantic Anomaly Detection and Explainable AI Approach." Risks 14.4 (2026): 87.

Yang, Z., Ji, W., Guo, Q., & Wang, Z. (2023, October). Javp: Joint-aware video processing with edge-cloud collaboration for dnn inference. In Proceedings of the 31st ACM International Conference on Multimedia (pp. 9152-9160).

Ma, Y., Qu, D., & Wang, Y. (2026). HALO-GNN: hallucination-resistant temporal graph neural networks for dynamic community detection.Scientific Reports.

Zhao, Q., & Huang, Y. (2026). DAREA: A Dynamic AI-Driven Architecture for Real Estate Asset Tokenization on Blockchain.Fundamental Scientific Reports in Multidisciplinary Areas,2(02), 182-192.

Li, X., Wang, P., Li, G., Ni, L., & Zhang, Y. (2023). Design of interface circuits and lightweight PUF for TMR sensors. IEEE Sensors Journal, 23(11), 11754-11761.

Li, X., Wang, P., Li, G., & Zhang, Y. (2023). Design of a novel self-test-on-chip interface ASIC for capacitive accelerometers. IEEE Transactions on Circuits and Systems I: Regular Papers, 70(7), 2834-2843.

Wang Y, Fang Y, Wang T, et al. Dreamnav: A trajectory-based imaginative framework for zero-shot vision-and-language navigation[J]. arXiv preprint arXiv:2509.11197, 2025.

Issa, M. A., Chen, H., Wang, J., & Imani, M. (2024). CyberRL: Brain-inspired reinforcement learning for efficient network intrusion detection.IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,44(1), 241-250.

Yao, Y., Zhao, J., Li, Z., Cheng, X., & Wu, L. (2023). Jamming and eavesdropping defense scheme based on deep reinforcement learning in autonomous vehicle networks. IEEE Transactions on Information Forensics and Security, 18, 1211-1224.

Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). Why should I trust you?: Explaining the predictions of any classifier. In Proceedings of KDD.

Li, X., Yin, L., Chen, W., Gao, Z., & Liu, X. (2017). A high-resolution tunneling magneto-resistance sensor interface circuit.Modern Physics Letters B,31(04), 1750030.