JURNAL INFOTEL
VOL. 17, NO. 2, MAY 2025, PP. 210–228. DOI:10.20895/INFOTEL.V17I2.1236

RESEARCH ARTICLE

Enhancing IoT Security: Optimizing PUF Responses through Pre-Processing Techniques

Fachrul Reiza Medina[1] and Parman Sukarno[2*]

[1,2]School of Computing, Telkom University, Indonesia

*Corresponding email: psukarno@telkomuniversity.ac.id

Received: August 31, 2024; Revised: March 04, 2025; Accepted: April 19, 2025.

Abstract: In this paper, we propose and detail the implementation of preprocessing techniques—specifically, truncation and uniformization to enhance the performance of authentication processes utilizing Physical Unclonable Functions (PUFs) within the Internet of Things (IoT) context. PUF technology addresses the problem of static secret storage in IoT by dynamically generating keys. However, despite the dynamic nature of PUF-generated secret keys, prior research has not focused on optimizing the secret keys generated by PUFs, resulting in a lack of additional security layers and maintaining susceptibility to PUF-targeted attacks at a constant level. This study introduces a PUF-based IoT device framework that optimizes PUF responses to significantly improve the security performance of the system. This enhancement is evaluated through metrics such as the decidability index (d), the confusion matrix, and the randomness value, presenting a comprehensive approach to strengthening the security of the system. Optimization of PUF responses through methods of truncation or bit uniformization plays a critical role in enhancing the security of IoT devices. Our findings indicate that bit uniformization significantly improves system security, evidenced by a significant increase in d' from 0.73 (unoptimized) to 1.37. This improvement is also reflected in the confusion matrix, with the False Rejection Rate (FRR), False Acceptance Rate (FAR), True Rejection Rate (TRR), and True Acceptance Rate (TAR) showing marked improvements from 18. 02%, 4. 93%, 95. 06% and 81. 97% in the unoptimized state at 3. 04%, 0. 98%, 99. 02%, and 96. 96%, respectively, after optimization. The proposed preprocessing techniques show their effectiveness in the PUF authentication systems used for IoT, as superior results are obtained.

Keywords: authentication, internet of things (IoT), physical unclonable function (PUF), preprocessing, security, truncation, uniformization

 ISSN: 2085-3688; e-ISSN: 2460-0997

1 Introduction

The Internet of Things (IoT) represents a paradigm in which devices are interconnected, facilitating communication between themselves, with edge networks, or through cloud-based platforms, leveraging open standard interoperable communication protocols for processing [1] [2]. The proliferation of IoT devices has been remarkable, with projections suggesting that by 2025, the average number of devices per individual could rise to 14.46, propelling the global IoT market to an anticipated value of $1.567 billion [3] [4]. Integrating IoT technology, especially in scenarios involving transmitting sensitive or personal data or deploying unmanned remote devices, underscores a pivotal concern for data and information security due to vulnerabilities such as unauthorized physical access to device memory. The criticality of ensuring that only authenticated and authorized IoT devices can transmit data cannot be overstated, given the paramount importance of protecting data privacy within these networks. Consequently, establishing a secure, reliable, and scalable authentication framework emerges as a fundamental requirement in implementing IoT technologies. This approach is essential to maintain the integrity and confidentiality of data in the vast and diverse landscape of IoT applications, ensuring that the vast potential of IoT can be realized safely and effectively [5].

The traditional methodology used in authentication mechanisms exhibits numerous deficiencies, mainly due to the static nature of secret storage. Embedding a static secret key within non-volatile storage mediums, such as fuses or EEPROM, and leveraging cryptographic methodologies, including digital signatures and encryption, for verifying device authenticity and protecting sensitive information presents significant financial and security management challenges. Specifically, the secure management of secret keys becomes increasingly problematic. Moreover, non-volatile memory technologies are inherently vulnerable to invasive attacks, given that secrets are preserved in digital format. Even in scenarios where battery-backed RAMs are used, there exists the potential for secret keys to be compromised after prolonged storage durations [3-5]. To achieve an elevated level of physical security, it is often necessary to implement expensive tamper-detection mechanisms that guard the integrated circuit, requiring a continuous power supply for their operation [6] [7] [8]. Furthermore, the adoption of secure hardware components, such as Hardware Security Modules (HSM) and Trusted Platform Modules (TPM), is frequently impractical within the context of IoT devices, which are constrained by limited resources, including available power and physical space [6]. Furthermore, an additional layer of security is needed to increase resilience and complexity against attacker attacks, including, for example, hardware hacking [9].

To reduce reliance solely on the secret key from the PUF, an additional secret key has been used as an external noisy source. However, previous studies, such as [10], did not optimize the PUF secret key, leaving it vulnerable to PUF attacks. This research introduces a PUF-based IoT device with optimized PUF responses to improve security. To achieve this, it is crucial to optimize the original PUF dataset. It is important to note that optimizing this dataset may also benefit attacker PUF datasets, unless the optimization is explicitly performed during the genuine PUF staging phase. The optimization method involves truncating or uniforming bits, with uniforming bits showing significant results in decidability value and separation between genuine and attacker noisy sources. Optimizing the secret key of the PUF (PUF responses) is essential to prevent attacks on PUF devices. This adds an additional security layer, ensuring that the authenticity of the PUF response data does not

rely solely on the secret key generated by the PUF. This optimization involves processing bits of PUF responses that significantly impact the quality of security parameters. Optimizing the PUF response dataset must address various PUF attacks and reduce reliance on the authenticity of the secret key based only on the dynamics of the PUF device.

The quantitative goal of this research is to improve system performance parameters, such as higher true acceptance and rejection rates and lower false acceptance and rejection rates. The decidability index, which determines if the noisy sources are authentic, needs to be enhanced. This can be achieved through various data processing schemes applied to data bits, which require the examination of randomness values in this study. This research introduces and validates preprocessing techniques, specifically truncation and uniformization, to optimize PUF responses, significantly improving the security performance of IoT authentication systems.

2 Review of Physical Unclonable Function

PUF serves as a foundational security component that leverages the intrinsic physical characteristics of an entity to generate a secret key for use in various security contexts [11] [12] [13]. The unique aspect of PUFs lies in their exploitation of the natural variability inherent in manufacturing processes, which makes duplication of a PUF extremely difficult, if not impossible, for potential adversaries. PUFs operate by receiving specific inputs, challenges, or stimuli and generating corresponding outputs called responses. Upon receiving a challenge, a PUF consistently delivers a precise response. The collection of these input-output pairs is known as Challenge-Response Pairs (CRPs). For a PUF to be considered adequate, it must fulfill several criteria: it should produce unique responses to different challenges, making it virtually impossible to predict a response without direct access to the PUF itself, and any attempt to uncover its internal structure would require modifications to the PUF's configuration, thereby altering its physical properties and, consequently, its challenge-response behavior. This feature effectively safeguards PUFs against cloning attempts. An illustration of the challenge-response mechanism employed by a PUF is shown in Figure 1 [14] [15].

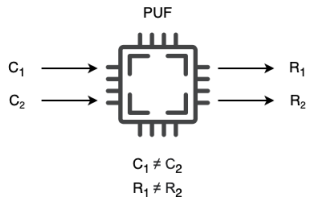

Figure 1: PUF challenge & response pair (CRP).

PUFs are categorized into various types, each defined by the unique attributes of the underlying hardware. Among these, some PUFs are designed to utilize the delay latency inherent in the propagation of data bit streams within electrical circuits. In addition, several PUFs capitalize on the intrinsic properties of specific components, including ring oscillators and memory systems. This study focuses on the Arbiter PUF (A-PUF), a widely recognized variant based on the differential delay latency encountered by data bits during

transmission. The A-PUF's reliance on timing discrepancies as a source of unpredictability exemplifies its innovative use of physical phenomena for security purposes, highlighting its significance in the landscape of PUF technologies.

2.1 Authentication Decidability

In the domain of authentication mechanisms [16], which adjudicate access authorization, performance is quantitatively assessed through a confusion matrix that encompasses four primary metrics: False Acceptance Rate (FAR), False Rejection Rate (FRR), True Acceptance Rate (TAR), and True Rejection Rate (TRR). These metrics are critical in evaluating the efficacy and reliability of an authentication system. The FAR, indicative of the incidence where unauthorized individuals are erroneously granted access, and the FRR, reflecting the instances of legitimate users being unjustly denied access, represent the error dimensions imperative to minimize. The optimal authentication system is characterized by low FAR and FRR values, which signify minimal security breaches and user inconvenience. FAR is synonymous with Type 1 error, while FRR correlates with Type 2. Furthermore, the interaction and balance between these rates and TAR and TRR can be visually analyzed through a Hamming distance graph, as illustrated in Figure 2. This graphical representation helps to understand the trade-offs between security and usability within the system [17].

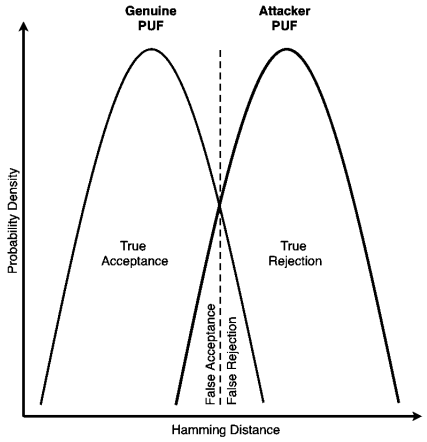

Figure 2: Landscape of authentication decision process.

The graphical representation of two distributions, delineating the distinction between authentic PUF access attempts and those simulated by attackers, provides a nuanced understanding of the accuracy of authentication [17]. The x-axis of this graph measures the Hamming Distance, which quantifies the bit discrepancies between two binary strings, offering a metric for comparing their similarity. A dotted line within the graph serves as a demarcation threshold, determining the boundary at which patterns are considered either sufficiently similar (indicating the exact origin, albeit with minor distortions) or distinctly different. This threshold embodies the trade-off between security and accessibility: its positioning toward the left (indicating a more lenient assessment) or toward the right (signifying a stricter evaluation) directly influences the likelihood of each of the four possible outcomes: True Acceptance, False Acceptance, True Rejection, and False Rejection.

The concept of "decidability" in an authentication context hinges on the extent of overlap between these two distributions. Enhanced “decidability,” or the ability to reliably discriminate between genuine and fraudulent access attempts is achieved when the means of the two groups diverge significantly or when their variances are minimized. A mathematical formula, referred to as Equation 1, offers one method for calculating the decidability index (*d'*) by incorporating the means and standard deviations of the two distributions under consideration. Although this equation is a valuable tool for quantifying "decidability," it represents just one of several approaches to assessing the effectiveness of an authentication system in distinguishing between legitimate and illegitimate access attempts based on PUF-generated data.

$$d' = \frac{|\mu_1 - \mu_2|}{\sqrt{\frac{1}{2}\left(\sigma_1^2 + \sigma_2^2\right)}}, \tag{1}$$

where μ_1, μ_2 and σ_1, σ_2 are the means and standard deviation of each graph distribution, respectively.

2.2 PUF Randomness

For a PUF chip to be considered effective, it must exhibit a balanced propensity to generate bits 0 and 1, ensuring an equal probability of occurrence for both outcomes [18]. This characteristic, called randomness, is an intrinsic quality of the PUF chip, indicative of the uniform distribution of bits 0 and 1 within the chip’s responses. The concept of randomness within the context of a PUF chip emphasizes the importance of equilibrium in the generation of cryptographic keys or other security-related outputs, where predictability would undermine the efficacy of security [19].

The measure of randomness, particularly the balance between bits 0 and 1, can be quantified by the relative frequency of the appearance of bit 1 in all responses produced by the PUF chip [20]. This mathematical expression of randomness, focusing on the prevalence of bit 1, is crucial for assessing the PUF chip’s suitability for security applications, where unpredictability and uniform distribution of binary outputs are paramount. The formula to calculate this relative frequency considers the total number of bit 1 occurrences within the aggregate of generated responses, providing a direct measure of the PUF chip’s randomness and, by extension, its reliability and security potential, and is expressed as follows:

$$p = \frac{1}{KL} \sum_{k=1}^{K} \sum_{l=1}^{L} b_{k,l}, \tag{2}$$

with p and K representing the relative frequency of bit 1 in all responses and the total number of responses generated from the PUF chip, and L denoting the response length. In contrast, k and l refer to the response k-th and the position l-th bit in the response of the PUF chip, respectively.

Subsequently, the level of randomness in the PUF chip is defined as follows:

$$H = -\log_2 \max(p, 1-p), \tag{3}$$

where $\log_2(0) := 0$. To assess the randomness of a bit sequence, H is defined based on min-entropy, as PUF outputs are anticipated to exhibit uniform distribution. H reaches its peak

at 1 when $p = 0.5$ and hits the lowest point at 0 when $p = 0$ or $p = 1$. The best p is 0.5 for a binary system, as it produces the maximum entropy of 1 bit and represents the maximum uncertainty or randomness in a system. It also provides the strongest unpredictability and ensures resilience against cloning and prediction.

2.3 Confusion Matrix

The confusion matrix is a pivotal instrument within statistical methodologies, facilitating the evaluation of the performance of a classification algorithm [17]. In the realm of access control mechanisms responsible for determining access rights, performance is rigorously evaluated using a confusion matrix comprising four key metrics: False acceptance rate (FAR), false rejection rate (FRR), true acceptance rate (TAR), and true rejection rate (TRR). These metrics, collectively called the confusion matrix, play a vital role in assessing the effectiveness and dependability of an authentication system. FAR indicates instances where unauthorized individuals are mistakenly granted access, while FRR reflects cases where legitimate users are unfairly denied access, highlighting crucial error dimensions that must be minimized. An ideal authentication system maintains low FAR and FRR values, indicating minimal security breaches and user inconvenience. The formula for each metric is shown as follows:

$$\text{FRR} = \frac{\text{Number of False Rejections}}{\text{Total Number of Genuine Attempts}} \times 100\%$$

$$\text{FAR} = \frac{\text{Number of False Acceptances}}{\text{Total Number of Impostor Attempts}} \times 100\%$$

$$\text{TRR} = \frac{\text{Number of True Rejections}}{\text{Total Number of Impostor Attempts}} \times 100\%$$

$$\text{TAR} = \frac{\text{Number True Acceptances}}{\text{Total Number of Genuine Attempts}} \times 100\%$$

The application of a confusion matrix in assessing the effectiveness of an authentication system underscores its utility in quantifying the system's capability to distinguish between legitimate access and potential security breaches. The distribution of values within the confusion matrix directly influences the calculation of the decidability index, reflecting the system's robustness and the reliability of its classification mechanisms. This, in turn, provides a comprehensive overview of the system's operational strengths and potential vulnerabilities, informing efforts to enhance its security posture.

2.4 Hamming Distance

The Hamming distance [21], in the context of PUFs, serves as a critical metric to evaluate the degree of dissimilarity between two responses generated by a PUF. Given that PUFs derive their responses from the unique physical characteristics of the underlying hardware, it is natural for these responses to exhibit slight variations or noise, even when the same input or challenge is applied. The Hamming distance is determined by counting the number of bit positions at which the two responses diverge, effectively measuring how many bits need to be altered to perfectly align the responses [17].

A minimal Hamming distance indicates a strong congruence between the expected and actual responses, suggesting that the PUF consistently reproduces a specific output in response to a given input. Conversely, a substantial Hamming distance points to notable response variations, which could signal issues with the PUF's reliability or external factors influencing its output.

The terminology around Hamming distance further distinguishes between intra-PUF and inter-PUF comparisons. The intra-PUF Hamming distance refers to the dissimilarity measure within the responses of a single PUF, highlighting the internal consistency or variability of the PUF. On the other hand, the inter-PUF Hamming distance compares the responses between two different PUFs, offering a gauge of the uniqueness and distinguishability of each PUF's responses. Both measures are pivotal for understanding and enhancing the security capabilities of PUF-based systems.

3 Proposed Design

3.1 Genuine PUF Design

This study integrates an Arbiter-based Physical Unclonable Function (A-PUF) characterized by a dual chain architecture with 128 stages. It incorporates a single D-Flip Flop to represent a Genuine PUF, indicative of an authentic user's device. Each stage within the A-PUF architecture is designed around 2-to-1 multiplexer (MUX) devices, which accept two inputs, designated as A and B, and generate an output, Y. The determination of the output Y is contingent upon the state of the input signal S, which in this set-up is derived from the challenge bits. The challenge bits are provided as an n-bit length input, which align with the requirements of the A-PUF to process and respond to the challenge.

3.2 Attacker PUF Design

In the research, the approach to simulating an attacker's PUF is executed through Python, specifically leveraging tools designed for this purpose. The simulation focuses on recreating the delay paths characteristic of an arbiter PUF, incorporating predefined noise levels to mimic real-world imperfections and variations. This aspect of the simulation is crucial to accurately representing the challenges associated with replicating the unique response patterns of a genuine PUF, which are inherently influenced by physical properties and manufacturing inconsistencies.

The simulation of the attacker PUF utilizes the pypuf library, a specialized Python library developed to experiment with and analyze PUFs. The configuration set for this simulated attacker PUF consists of four chains, each comprising 128 stages, as shown in Figure 3. This configuration is designed to reflect a complex setup that an attacker might employ to clone or replicate the responses of a genuine PUF.

The pypuf library provides a robust framework for the simulation, enabling the research team to model the behaviour of arbiter PUFs under various conditions meticulously. By adjusting the noise levels and experimenting with different configurations, such as the four-chain setup, the team can explore the resilience of PUF technology against sophisticated attack strategies. This approach helps to understand the potential vulnerabilities of PUF-based security systems and contributes to developing more secure and reliable PUF implementations in the future [1].

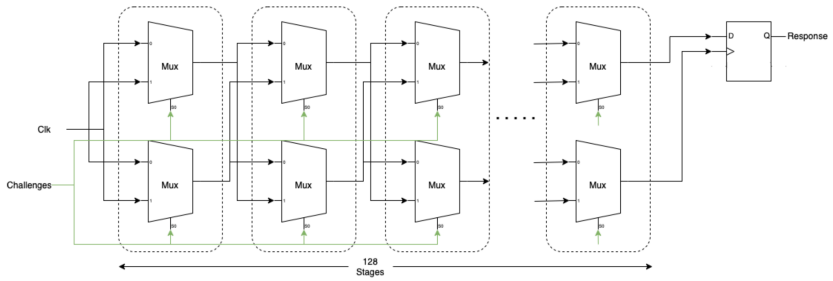

Figure 3: Attacker PUF design

3.3 CRPs Dataset Generation & Optimization

In generating responses to the presented challenges, the unique operational characteristic of the Arbiter PUF, producing a single-bit response for each 128-bit challenge, is central to the process. Compiling a complete 128-bit response requires 128 iterations per challenge, ensuring a complete response set is formed. Upon accumulating 1000 CRPs from both Genuine and Attacker PUFs, the focus shifts towards optimizing the Genuine PUF dataset through preprocessing techniques.

The preprocessing process aims to refine the Genuine PUF dataset to enhance authentication decidability, which is principally assessed through the Hamming distance plot contrasting the Genuine and Attacker PUF datasets. The objective is to diminish any overlap within the inter-Hamming distance distribution between the two datasets, thereby reducing the False Acceptance Rate (FAR) and False Rejection Rate (FRR). By meticulously optimizing the Genuine PUF dataset, the research strives to bolster the authentication system's resilience, achieving a more secure and reliable mechanism for distinguishing between authentic and fraudulent access attempts. This preprocessing technique seeks to minimize potential security vulnerabilities and increase the overall efficacy of the PUF-based authentication framework.

The preprocessing of the Genuine PUF dataset is approached through two distinct methodologies: truncating bits and uniforming bits. The truncated bits method scrutinizes the specific bit positions that contribute predominantly to the Hamming distance, essentially, locations where the bits most frequently diverge during comparisons. The method aims to exclude these particularly variable bits from the authentication process by identifying these positions. This exclusionary process naturally reduces the length of the PUF response, which, although initially comprising 128 bits, may result in a shorter bit sequence post-optimization. The bits targeted for removal are those identified as having the highest frequency of variance in their values during the calculation of Hamming distances, thereby streamlining the response by eliminating elements that introduce the most noise or inconsistency into the authentication mechanism.

This preprocessing technique is based on the premise that removing the bits most susceptible to variability can significantly improve the overall reliability and decisiveness of the PUF-based authentication system. The rationale is straightforward: By eliminating the primary sources of discrepancy, the system can achieve a more stable and predictable set of responses, which, in turn, facilitates a more accurate and secure authentication process. This approach underscores a strategic trade-off between the response data's comprehen-

siveness and the authentication outcome's precision, aiming to maximize security efficacy by minimizing potential points of vulnerability within the dataset.

The uniforming bits method represents an alternative approach to optimizing the Genuine PUF dataset, focusing on enhancing the system's decisiveness without excluding bits from the authentication process. Like the method of the truncating bit, this technique involves a detailed analysis of bit positions that have a pronounced impact on the Hamming distance, specifically those that exhibit the most significant variability during comparisons. However, rather than removing these bits, the uniforming bits method seeks to normalize their values, standardizing them to a consistent value, typically zero.

This standardization process aims to reduce the variability and noise within the dataset, thereby improving the authentication system's ability to differentiate between genuine and attacker PUF responses decisively. By aligning the values of the most variable bits, the method effectively reduces the entropy of the dataset, which denotes a decrease in randomness. While this reduction in randomness compromises the system's security, the trade-off is acceptable if it results in a significant enhancement of the decidability value, thus bolstering the overall efficacy of the authentication process.

Certain safeguards can be implemented to mitigate the potential security risks associated with decreased entropy. One such measure is to restrict the authentication attempts to a maximum of three tries, thereby limiting the opportunities for unauthorized access attempts to exploit the reduced randomness of the dataset. This limitation is a strategic counterbalance, ensuring that an increased vulnerability to systematic attack methodologies does not undermine the benefits gained in authentication feasibility and system robustness. Through carefully applying and balancing these optimization techniques, the authentication system can achieve an optimal blend of security, reliability, and performance.

The illustration of the optimization process for the Genuine PUF dataset is as follows:

1. Suppose that there are three genuine PUF responses, each of which is 8 bits long (it should be noted that the length of the PUF response in the original dataset is 128 bits). The three responses are 11011001, 10111010, and 00110100, respectively.
2. The Hamming distance calculation is performed by comparing the first PUF respoiterations the second PUF response, the first PUF response with the third PUF response, and the second PUF response with the third PUF response (in the original dataset with 1000 CRPs, the Hamming distance calculation involves comparing the first PUF response with the second PUF response, the first PUF response with the third PUF response, ..., the first PUF response with the 1000th PUF response, the second PUF response with the third PUF response, and so on, until the comparison process between the 999-th PUF response and the 1000-th PUF response).
3. The results of the first, second, and third iteration are illustrated in Figure 4, Figure 5, and Figure 6, respectively.
4. Based on the results of the last iteration, it can be observed that the positions of bits that most frequently differ are the positions of bits 2_{nd}, 3_{rd}, and 5_{th}. Subsequently, these bits can be eliminated if the truncating method is used. For example, the PUF responses are initially 11011001, 10111010, and 00110100. Because the positions of bits number 2_{nd}, 3_{rd}, and 5_{th} contribute the most to the Hamming distance, the bit positions from these responses can be eliminated. Thus, the PUF responses become 1011001, 1111010, and 0110100 (if only eliminating the position of bit number 2_{nd}), the PUF responses become 111001, 111010, and 010100 (if eliminating the positions

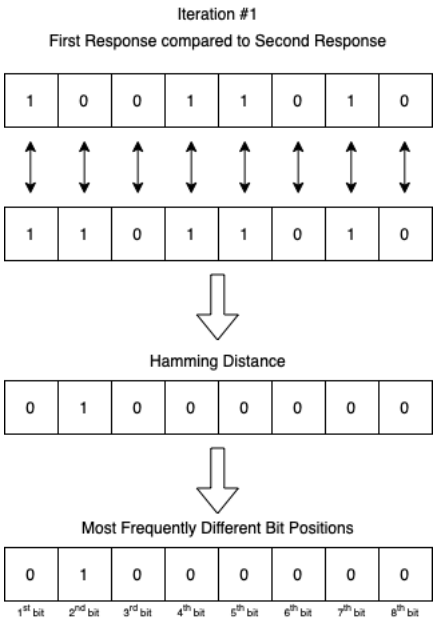

Figure 4: Illustration #1 of optimizing genuine PUF dataset.

of bits number 2_{nd}, 3_{rd}), and the PUF responses become 11001, 11010, and 01100 (if eliminating the positions of bits number 2_{nd}, 3_{rd}, and 5_{th}).

5. Also, when the uniforming method is used, these bits can be "uniformed." For example, the PUF responses are initially 11011001, 10111010, and 00110100. Because the positions of bits number 2_{nd}, 3_{rd}, and 5_{th} contribute the most to the Hamming distance, the bit positions from these responses can be uniform. Thus, the PUF responses become 10011001, 10111010, and 00110100 (if only uniforming the position of bit number 2_{nd}), the PUF responses become 10011001, 10011010, and 00010100 (if eliminating the positions of bits number 2_{nd}, 3_{rd}), and the PUF responses become 10010001, 10010010, and 00010100 (if eliminating the positions of bits number 2_{nd}, 3_{rd}, and 5_{th}). Notice that the PUF response length remains the same.

4 Experimental Result and Evaluation

In the presented research, two datasets of Challenge-Response Pairs (CRPs), each containing 1000 entries, were used to represent the responses from genuine and attacker PUF devices. This dual data set approach is crucial to assess the robustness and security of PUF-based authentication systems under real-world conditions where legitimate users and potential attackers are present.

By comparing and contrasting these two datasets, the research strives to validate the security and uniqueness of genuine PUF responses, explore potential vulnerabilities, and

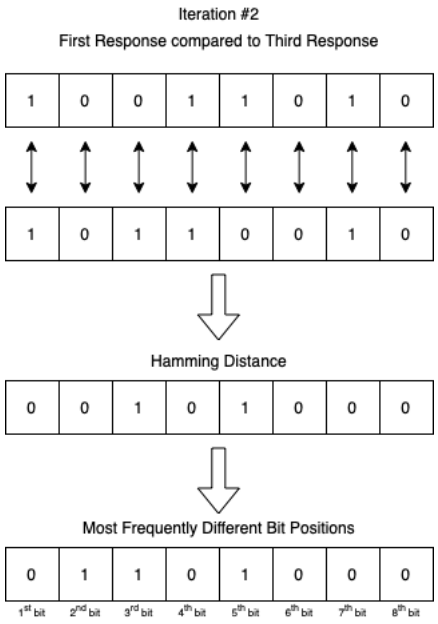

Figure 5: Illustration #2 of optimizing genuine PUF dataset.

strengthen the overall reliability of PUF-based authentication systems against emulation attempts.

Optimizing the original PUF dataset is essential for attaining optimal performance in authentication systems. However, it is important to acknowledge that the optimization techniques applied to the genuine PUF dataset might inadvertently benefit the attacker's PUF dataset, mainly if the optimization process enhances specific characteristics that could be mimicked or exploited by an attacker. Therefore, optimization efforts should ideally be conducted with awareness of this potential issue, incorporating measures to ensure that any optimizations applied during the staging phase of the genuine PUF do not simultaneously facilitate the task of attackers. This careful balance act is crucial for maintaining the security integrity of PUF-based authentication systems while striving for improved performance and reliability.

4.1 Unoptimized PUF's Secret Key Dataset Performance

In this subsection, we analyze intra-PUF and inter-PUF parameters before any optimization is applied to the genuine PUF dataset. This analysis is pivotal for establishing a baseline understanding of the PUF's performance characteristics, which, in turn, informs the subsequent optimization efforts. The Hamming distance plot is illustrated in Figure 7, and the randomness and decidability values, along with parameters that represent the characteristics of the hamming distance between and between the hammers, are presented in Table 1. Furthermore, the confusion matrix is displayed in Table 2.

Moreover, the positions of bits most frequently have different values when calculating the hamming distance, as indicated in Figure 8. Figure 8 shows that the bit positions fol-

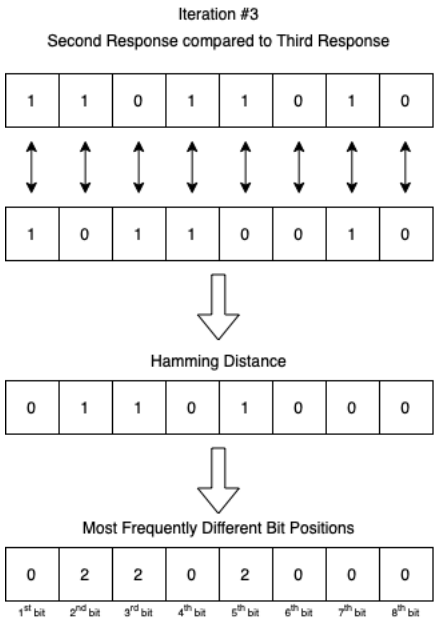

Figure 6: Illustration #3 of optimizing genuine PUF dataset.

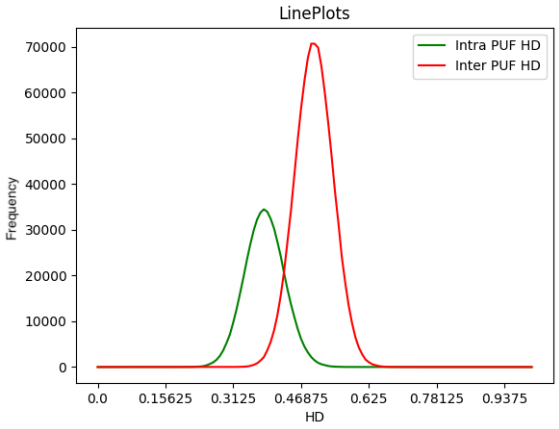

Figure 7: Unoptimized genuine PUF dataset - Hamming distance plot.

lowing 60 have the highest inconsistency values. This can lead to a high False Rejection Rate (FRR), where genuine data is mistakenly rejected. Therefore, a strategy should be implemented to conceal these inconsistent bits.

Table 1: Randomness & Hamming distance plot parameters

No	Parameter	Value	Remark
1	Randomness	70.94%	-
2	Mean	51.57	Intra-PUF, unnormalized
3	Standard Deviation	15.72	Intra-PUF, unnormalized
4	Mean	63.06	Inter-PUF, unnormalized
5	Standard Deviation	15.39	Inter-PUF, unnormalized
6	Decidability Index	0.73	-

Table 2: Confusion matrix

	Acceptance Rate	Rejection Rate
True	81.98%	95.06%
False	4.94%	18.02%

4.2 Optimized PUF's Secret Key Dataset Performance

Optimization strategies for PUF datasets, specifically truncating bits and uniformizing bits, employ different methodologies to enhance the performance and security of PUF-based authentication systems. Both approaches aim to improve the decidability and reliability of PUF responses but impact the dataset's characteristics in distinct ways.

The research incorporates an experimental approach. It optimizes 4, 8, 12, and 16 bits within the PUF responses to evaluate the impact of different levels of optimization on the system's performance. Determining which bits to optimize is done during the staging phase based on analyzing the genuine PUF response dataset.

This methodical exploration of optimization levels aims to identify the optimal balance between maintaining sufficient randomness (to ensure security) and enhancing decidability (to ensure reliable authentication). By comparing the effects of truncating versus uniformizing bits across various degrees of optimization, the research seeks to delineate best practices for refining PUF datasets, thereby contributing valuable insights to the field of hardware-based security.

When considering the impact of optimization processes on PUF response data, two distinct scenarios emerge, as delineated in Figure 9 and Figure 10. In Figure 9, optimization, specifically preprocessing of bit values within PUF responses, can either singularly affect genuine PUF responses or concurrently influence genuine and attacker PUF responses. This distinction depends on the phase during which the optimization is implemented.

If optimization occurs during the staging phase, a preliminary stage involving generating and registering the PUF dataset within the system, then the preprocessing modifications are applied solely to genuine PUF responses. Consequently, in the subsequent production phase, which encompasses the enrollment and reproduction stages of the authentication system, only these preprocessed genuine PUF responses are subject to the effects of optimization.

Conversely, should optimization be undertaken exclusively during the production phase, without preceding bit preprocessing during the staging phase, the modifications indiscriminately affect all PUF responses, irrespective of their origin. This approach stems from the inherent ambiguity during the production phase regarding the legitimacy of the

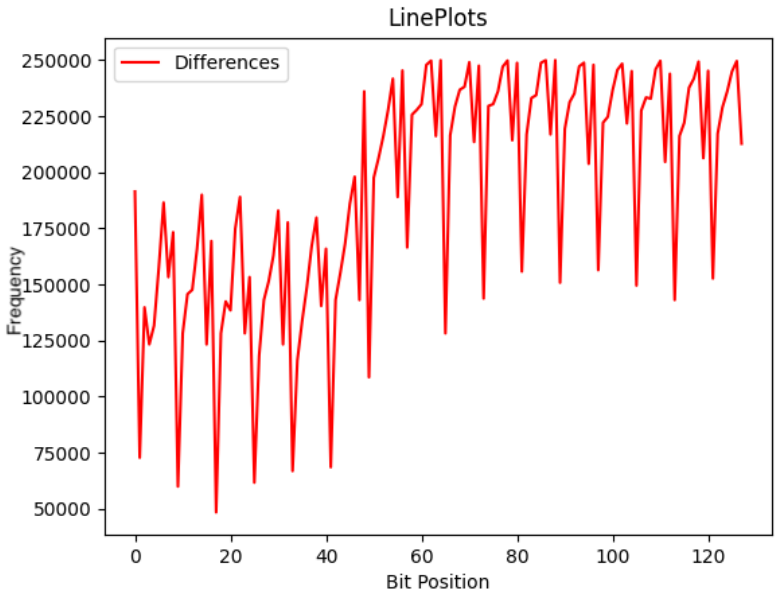

Figure 8: Frequency of bit differences in Hamming distance calculation.

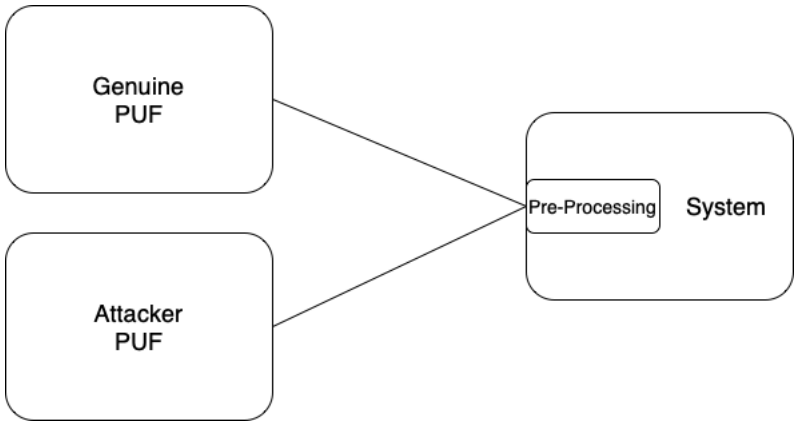

Figure 9: Centralized preprocessing response bits (dataset optimization).

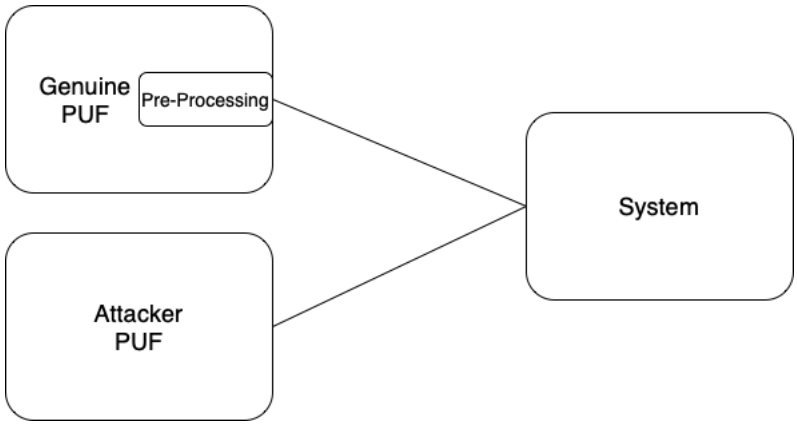

Figure 10: Distributed preprocessing response bits (dataset optimization).

responses, rendering it impossible to differentiate between genuine and attacker-derived PUF responses. As a result, optimization during this phase extends to the entire spectrum of PUF responses.

However, it is pertinent to note that optimization during the staging phase allows for the verification of the PUF response dataset's authenticity, ensuring that bit preprocessing is selectively applied to genuine PUF responses. This strategy underscores the importance of the optimization timeline in preserving the integrity and security of PUF-based authentication systems.

Meanwhile, the illustration in Figure 10 shows distributed pre-processing of bits, which affects only genuine PUF responses. In particular, the preprocessing in Figure 9 occurs not only during the production phase (enrollment and reproduction phases), but also during the staging phase of genuine PUF.

Based on the outlined considerations, it is deduced that optimizing the PUF response dataset, utilizing the truncating bits method, aligns with a centralized bit preprocessing paradigm. This model predicates that bit preprocessing occurs exclusively within a centralized framework. In contrast, the optimization employing the uniforming bits method aligns with a distributed bit preprocessing paradigm, where the preprocessing of bits is executed at each remote Internet of Things (IoT) device rather than being centralized.

The rationale for the infeasibility of a distributed preprocessing model in conjunction with the truncated bits method lies in the potential ease with which attackers can discern the optimization of the PUF response dataset. Specifically, attackers might more readily identify the bit preprocessing due to discrepancies in key lengths when attempting system access with a 128-bit extended PUF response. Conversely, the application of the uniform bit method within a distributed preprocessing framework does not afford attackers immediate insights into the existence of preprocessing, as the system's feedback to unauthorized access attempts does not include key-length discrepancies, merely indicating incorrect key entries.

Moreover, applying uniform bits within a centralized pre-processing model is somewhat redundant. This is because its performance outcomes are anticipated to closely mirror those achieved through the truncating bits method under a centralized preprocessing

Table 3: Summary PUF dataset optimization performance

No	Optimization	d'	H	FRR	FAR	TRR	TAR
1	Unoptimized	0.73	70.94%	18.02%	4.93%	95.06%	81.97%
2	Truncated, 4-bits	0.80	71.6%	17.59%	4.70%	95.29%	82.41%
3	Truncated, 8-bits	0.81	72.25%	17.21%	4.47%	95.53%	82.79%
4	Truncated, 12-bits	0.76	72.90%	12.75%	6.23%	93.77%	87.25%
5	Truncated, 16-bits	0.82	73.56%	12.33%	5.81%	94.19%	87.67%
6	Uniformed, 4-bits	0.99	69.36%	10.2%	3.66%	96.34%	89.8%
7	Uniformed, 8-bits	1.08	67.74%	7.09%	2.26%	97.74%	92.91%
8	Uniformed, 12-bits	1.13	66.06%	4.75%	1.78%	98.22%	95.25%
9	**Uniformed, 16-bits**	**1.37**	**64.36%**	**3.04%**	**0.98%**	**99.02%**	**96.96%**

model, given the optimization's substantial impact on genuine and attacker PUF response datasets. The cumulative results of the PUF response dataset optimization process, employing both truncating and uniforming bits methods within this research framework, are encapsulated in Table 3. This summary elucidates the nuanced implications of each optimization strategy, underscored by their operational paradigms, and the consequent security implications for PUF-based authentication systems.

The optimization results using the truncated bits method, which adopts a centralized preprocessing approach, reveal a lack of significant performance enhancements and do not demonstrate a linear relationship in performance improvement. In contrast, the optimization utilizing the uniform bits method, characterized by a distributed preprocessing framework, yields substantial performance gains and exhibits a linear improvement in performance metrics. This linearity suggests a consistent improvement in system reliability and security with each incremental optimization step.

Given these observations, this study advocates the adoption of the uniform bits method, specifically the uniformization of 16 bits, as the preferred optimization strategy. This preference is attributed to its superior decidability value and the most advantageous confusion matrix outcomes, characterized by the lowest false rejection rate and the highest true rejection rate, despite the compromised randomness value associated with this method. The diminished randomness, or entropy, is considered a manageable trade-off, given the pronounced improvements in decidability and confusion matrix outcomes.

Table 4: Randomness & Hamming distance plot parameters - uniformed 16 bits

No	Parameter	Value	Remark
1	Randomness	64.36%	-
2	Mean	43.0	Intra-PUF, unnormalized
3	Standard Deviation	14.72	Intra-PUF, unnormalized
4	Mean	63.5	Inter-PUF, unnormalized
5	Standard Deviation	15.01	Inter-PUF, unnormalized
6	Decidability	1.37	-

To mitigate the reduced randomness inherent to the uniforming 16-bit method, a controlled approach to authentication attempts by IoT devices is proposed. This control mech-

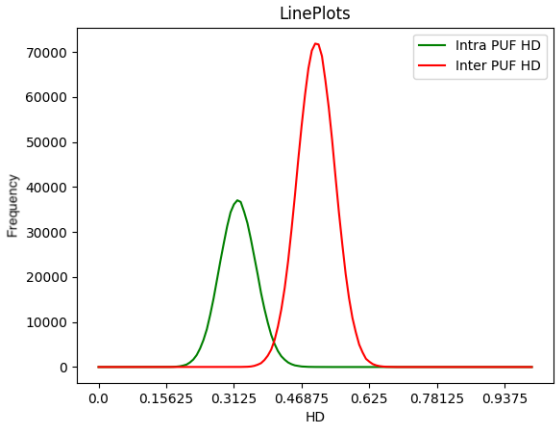

Figure 11: Optimized genuine PUF dataset, uniformed 16 bits.

anism balances the security implications of the decreased entropy without detracting from the overall effectiveness of the PUF-based authentication system. In the context of this research, while randomness is an important factor, it does not supersede the criticality of decisiveness and the confusion matrix in determining the optimization strategy's success.

The distinction between genuine PUF (intra-PUF) responses and Rogue or Attacker PUF (inter-PUF) responses is visually represented in Figure 11 and detailed in Table 4. This visualization and tabulation delineate the enhanced separation achieved through the 16-bit uniformization method, underscoring its efficacy in distinguishing between legitimate and fraudulent PUF responses. The clear demarcation between intra-PUF and inter-PUF responses highlights the optimization method's contribution to improving the authentication system's security and reliability.

5 Conclusion

Before the implementation of preprocessing techniques on PUF responses, the decisability metric stood at a modest 0.73, coupled with a relatively high False Rejection Rate (FRR) of 18.02% and a True Acceptance Rate (TAR) of merely 81.97%. Such figures underscore the insufficient delimitation between genuine and attacker PUF responses, thus compromising the authenticity and security of the PUF-based authentication process. Additionally, the vulnerability of unoptimized PUF data to various PUF-centric attacks further exacerbates the system's security shortcomings.

Upon the introduction of optimization techniques to the PUF responses, the uniformization of 16 bits emerged as the paramount method. This approach entails standardizing the most variable bit positions that exhibit the most significant differences during Hamming distance calculations in a subset of 16 bits. Implementing this optimization technique caused a notable improvement in the determinability value, increasing it to 1.37. This enhancement was accompanied by a marked reduction in the FRR to 3.04%, alongside a substantial uplift in the TAR to 96.96%. The resultant metrics signal a more pronounced

distinction between genuine and fraudulent biometrics, attributed to the substantial increase in the decidability value. Therefore, the outcomes derived from the uniform 16-bit optimization approach suggest significant effectiveness in the PUF authentication systems used for IoT, as superior results are obtained.

Future studies could increase the length of the key to achieve greater security performance. Furthermore, in the future, the proposed mechanism in this study can be tested with a more extensive and varied dataset of genuine and attacker-noisy sources.

Acknowledgments

The financial support of the Indonesia's DRTPM, DITJEN DIKTIRISTEK, KEMDIKBUDRISTEK through grant 106/E5/PG.02.00.PL/2024, 043/SP2H/RT-MONO/LL4/2024, and 090/LIT07/PPM-LIT/2024 is hereby acknowledged and appreciated.

References

[1] H. Ning, F. Farha, A. Ullah, and L. Mao, "Physical unclonable function: architectures, applications and challenges for dependable security," *IET Circuits, Devices & Systems*, vol. 14, no. 4, pp. 407–424, 2020.

[2] A. A. da Conceic'ão, L. P. Ambrosio, T. R. Leme, A. C. Rosa, F. F. Ramborger, G. P. Aquino, and E. C. V. Boas, "Internet of things environment automation: A smart lab practical approach," in *2022 2nd International Conference on Information Technology and Education (ICIT&E)*, pp. 01–06, IEEE, 2022.

[3] S. Al-Sarawi, M. Anbar, R. Abdullah, and A. B. Al Hawari, "Internet of things market analysis forecasts, 2020–2030," in *2020 Fourth World Conference on smart trends in systems, security and sustainability (WorldS4)*, pp. 449–453, IEEE, 2020.

[4] E. Korneeva, N. Olinder, and W. Strielkowski, "Consumer attitudes to the smart home technologies and the internet of things (iot)," *Energies*, vol. 14, no. 23, p. 7913, 2021.

[5] R. R. Pahlevi, P. Sukarno, and B. Erfianto, "Secure MQTT PUF-based key exchange protocol for smart healthcare," *J. Rekayasa Elektr.*, vol. 17, June 2021.

[6] E. Hunt-Schroeder and T. Xia, "Tamper resistant reconfigurable pre-amplifier physical unclonable function with self-destruct," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2024.

[7] K. Lounis and M. Zulkernine, "Lessons learned: Analysis of puf-based authentication protocols for iot," *Digital threats: research and practice*, vol. 4, no. 2, pp. 1–33, 2023.

[8] Y. Gao, S. F. Al-Sarawi, and D. Abbott, "Physical unclonable functions," *Nature Electronics*, vol. 3, no. 2, pp. 81–91, 2020.

[9] N. N. Anandakumar, M. S. Hashmi, and M. Tehranipoor, "Fpga-based physical unclonable functions: A comprehensive overview of theory and architectures," *Integration*, vol. 81, pp. 175–194, 2021.

[10] D. Choi, S.-H. Seo, Y.-S. Oh, and Y. Kang, "Two-factor fuzzy commitment for unmanned iot devices security," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 335–348, 2018.

[11] M. K. Ahmed, V. P. Yanambaka, A. Abdelgawad, and K. Yelamarthi, "Physical unclonable function based hardware security for resource constraint iot devices," in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, pp. 1–2, IEEE, 2020.

[12] Y. Zhang, B. Li, B. Liu, Y. Hu, and H. Zheng, "A privacy-aware pufs-based multiserver authentication protocol in cloud-edge iot systems using blockchain," *IEEE Internet of Things Journal*, vol. 8, no. 18, pp. 13958–13974, 2021.

[13] A. Yadav, S. Kumar, and J. Singh, "A review of physical unclonable functions (pufs) and its applications in iot environment," *Ambient Communications and Computer Systems: Proceedings of RACCCS 2021*, pp. 1–13, 2022.

[14] B. B. Talukder, F. Ferdaus, and M. T. Rahman, "Memory-based pufs are vulnerable as well: A non-invasive attack against sram pufs," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 4035–4049, 2021.

[15] F. Zerrouki, S. Ouchani, and H. Bouarfa, "Quantifying security and performance of physical unclonable functions," in *2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, pp. 1–4, IEEE, 2020.

[16] M. Golec, S. S. Gill, R. Bahsoon, and O. Rana, "Biosec: A biometric authentication framework for secure and private communication among edge devices in iot and industry 4.0," *IEEE Consumer Electronics Magazine*, vol. 11, no. 2, pp. 51–56, 2020.

[17] D. Palma and P. Luca Montessoro, "Biometric-based human recognition systems: An overview," in *Recent Advances in Biometrics*, IntechOpen, July 2022.

[18] M. Khalafalla and C. Gebotys, "Pufs deep attacks: Enhanced modeling attacks using deep learning techniques to break the security of double arbiter pufs," in *2019 Design, automation & test in Europe conference & exhibition (DATE)*, pp. 204–209, IEEE, 2019.

[19] S. Elgendy and E. Y. Tawfik, "Impact of physical design on puf behavior: a statistical study," in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1–5, IEEE, 2021.

[20] R. L. Sembiring, R. R. Pahlevi, and P. Sukarno, "Randomness, uniqueness, and steadiness evaluation of physical unclonable functions," in *2021 9th International Conference on Information and Communication Technology (ICoICT)*, pp. 429–433, IEEE, 2021.

[21] L. Metcalf and W. Casey, "Chapter 2 - metrics, similarity, and sets," in *Cybersecurity and Applied Mathematics* (L. Metcalf and W. Casey, eds.), pp. 3–22, Boston: Syngress, 2016.