IoT

MDPI

Article

A Distributed Lightweight PUF-Based Mutual Authentication Protocol for IoV

Mona Alkanhal [1,*], Abdulaziz Alali [2] and Mohamed Younis [1]

[1] Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore, MD 21250, USA; younis@umbc.edu
[2] Department of Electrical and Biomedical Engineering, University of Nevada, Reno, NV 89557, USA; abdulazizalali@unr.edu
* Correspondence: monaa1@umbc.edu

Abstract: In recent times, the advent of innovative technological paradigms like the Internet of Things has paved the way for numerous applications that enhance the quality of human life. A remarkable application of IoT that has emerged is the Internet of Vehicles (IoV), motivated by an unparalleled surge of connected vehicles on the roads. IoV has become an area of significant interest due to its potential in enhancing traffic safety as well as providing accurate routing information. The primary objective of IoV is to maintain strict latency standards while ensuring confidentiality and security. Given the high mobility and limited bandwidth, vehicles need to have rapid and frequent authentication. Securing Vehicle-to-Roadside unit (V2R) and Vehicle-to-Vehicle (V2V) communications in IoV is essential for preventing critical information leakage to an adversary or unauthenticated users. To address these challenges, this paper proposes a novel mutual authentication protocol which incorporates hardware-based security primitives, namely physically unclonable functions (PUFs) with Multi-Input Multi-Output (MIMO) physical layer communications. The protocol allows a V2V and V2R to mutually authenticate each other without the involvement of a trusted third-party (server). The protocol design effectively mitigates modeling attacks and impersonation attempts, where the accuracy of predicting the value of each PUF response bit does not exceed 54%, which is equivalent to a random guess.

Keywords: Internet of Things (IoT); Internet of Vehicles (IoV); physical unclonable functions (PUFs); authentication; physical layer security; Vehicle-to-Vehicle (V2V); Vehicle-to-Roadside (V2R); Multiple-Input Multiple-Output (MIMO)

Citation: Alkanhal, M.; Alali, A.; Younis, M. A Distributed Lightweight PUF-Based Mutual Authentication Protocol for IoV. *IoT* **2024**, *5*, 1–19. https://doi.org/10.3390/iot5010001

Academic Editor: Amiya Nayak

Received: 21 November 2023
Revised: 27 December 2023
Accepted: 28 December 2023
Published: 30 December 2023

1. Introduction

The Internet of Vehicles is a cutting-edge technology that has made significant strides by creating intelligent vehicles equipped with connected sensors and electronic control units (ECUs). Wireless communication has significantly transformed the way data are transmitted by enabling faster and more reliable connectivity with lower latency and higher availability [1]. These advances have been embraced by various protocols and applications in IoV [2]. In essence, IoV represents the integration of Vehicular Ad Hoc Networks (VANETs) and the Internet of Things (IoT) [3]. The emergence of IoT has resulted in a significant change in the way vehicles interact with networks to obtain real-time traffic updates, ensure safe navigation, and support other driving features. According to industry analysts at Gartner, the imminent arrival of the fifth-generation IoT communication technology (5G IoT) is expected to be the driving force behind the development of connected cars. It is projected that by 2030, the automotive industry will capture a substantial percentage of the market opportunity for 5G IoT, with connected vehicles accounting for approximately 53% of the overall 5G IoT endpoints [4].

IoV leverages a range of networking technologies to facilitate seamless communication between different components within a vehicle, as well as with other entities on the

road, such as other vehicles and the roadside infrastructure. This fosters the sharing of valuable insights and information. However, given the presence of multiple IoT sensors and processors within the IoV network, connectivity through the network does carry inherent risks. Wireless communications between vehicles and V2R generally make them vulnerable to a number of security attacks, including Denial of Service (DoS), masquerading, and man-in-the-middle attacks. An eavesdropper can overhear communications between a user and a vehicle. Consequently, a piece of secret information is captured and misused for different malicious purposes, which can cause serious interruptions [5]. Moreover, the constant exchange of information between road entities makes IoV an attractive target for eavesdroppers [6]. Such vulnerability raises significant concerns, as it can potentially lead to malicious activities that can endanger the safety, security, and privacy of the vehicle system. The manipulation of Tesla's Autopilot self-driving software by hackers is an example of how serious this issue is, where the software was tricked into swerving into oncoming traffic [7]. Given the security threats of IoV, protecting the network is very crucial.

Node (or user) authentication is an essential security aspect before launching a secure communication session. Most existing authentication protocols in IoV are cryptography based, either asymmetric (employing public–private keys), or symmetric (using a shared secret key) [8]. The former is computationally demanding for the resource-constrained vehicle on-board electronic system, while the latter requires key pre-agreement and storage and often involves a trusted third-party, e.g., a server. A centralized node authentication process would not suit V2V and V2R communication [9]. An effective hardware-based strategy that has been proposed in the literature is to generate authentication tokens (secret keys) dynamically [10]. PUFs are one example of hardware primitives that can support such a strategy. The PUF design makes use of the random and uncontrollable variations that occur during the manufacturing of integrated circuits to create a unique device signature. PUF is a technology that maps input bits, known as a challenge, to an output bit or bits that reflect the circuit output response. This unique challenge–response mapping is often exploited in security solutions as an alternative to storing secrets in device memories [11].

One of the primary benefits of PUF-based authentication is that it facilitates the generation of a secret key/token on demand, thereby eliminating the need for storage. Typically, a server is given a subset of the challenge–response pairs (CRPs). The server then acts as a verifier by sending the vehicle (prover) a challenge bit-string and matches what the prover generates from its PUF with the pre-known (expected) response. However, the aforementioned process is not compatible with environments like the IoV, which prefer autonomous management strategies. One major challenge with using PUFs for distributed authentication is that the exchange of challenge and response happens between IoV nodes instead of the secure server. This increases the vulnerability to attacks, as eavesdroppers can intercept these interactions and collect enough CRPs to model the underlying PUF using machine learning (ML) techniques [12]. Encrypting the challenge and/or the response imposes overhead and requires key management, and consequently is not an attractive option. This paper aims to address this technical issue by utilizing the physical properties of communication links to obscure the exchanged challenge and response bits between IoV nodes [13]. Specifically, we leverage the increased use of the MIMO technology in wireless communication. As shown in Figure 1, every node will have an embedded PUF as well as a MIMO antenna array.

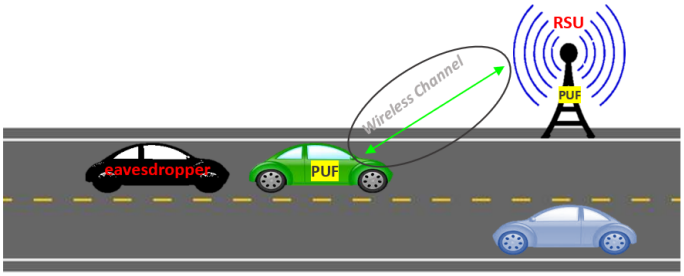


Figure 1. System model with a vehicle, RSU and an eavesdropper.

We propose a novel lightweight mutual authentication protocol for V2V and V2R without involving heavy computational techniques, such as cryptography-based algorithms. The proposed protocol obtains a node, i.e., a vehicle δ_A, to share a limited number of its CRPs $\gamma_{A\to B}$ with a roadside unit (RSU), i.e., verifier δ_B. Contrasted with a central network where a secure server is involved, a set $\gamma_{A\to B}$ might be disclosed or δ_B gets hacked. Our proposed protocol employs an innovative technique to prevent a cloning attack that might eavesdrop on the communication between δ_B and δ_A, thereby capturing a number of CRPs to model the δ_A PUF accurately. The challenge bit is encoded using the MIMO antenna array in a way that is controlled by the verifier and changes continuously. As demonstrated by the results of a PUF implementation, our proposed method effectively and robustly defeats cyberattacks. This paper extends our previous work [14] that exploits PUFs and MIMO in authenticating IoT nodes. Such work does not handle dynamic scenarios, where a node is in motion, which is common in the context of the IoV. The proposed protocol addresses such a limitation. To ease the presentation, we use δ_A as an indication of the vehicle throughout the paper and δ_B for the RSU node. The main contribution of this work can be summarized as follows:

- Developing a novel lightweight mutual authentication protocol for IoV that does not require a trusted third party, such as a server, during the authentication process;
- Leveraging hardware-based security primitives, specifically PUFs, which ensures no heavy computational overhead is imposed on the resource constraints of IoV;
- Exploiting the configurability of the MIMO technology to implicitly transmit the CRPs of the PUF and mutually authenticate the IoV nodes;
- Proposing a mapping technique that utilizes the physical properties of communication links to obscure the exchanged challenge and response bits between IoV nodes, thereby protecting against ML-based PUF modeling attacks and impersonation attempts.

The remainder of the paper is organized as follows. Section 2 discusses the related work on IoV authentication and PUF-based solutions. In Section 3, we cover some background on PUFs, present the system model, and provide an overview of our solution strategy. Section 4 describes the proposed protocol in detail. Sections 5 and 6 report the validation setup and performance results, while Section 7 provides an error rate analysis. We conclude the paper in Section 8.

2. Related Work

Numerous security provisions and authentication techniques have been developed to protect wireless networks [15]. Yet, these techniques fall short of the requirements for an IoV network that operates in an unattended setup with minimal human intervention. Storing the device identity in its memory, which is widely utilized in various authentication techniques, might not be sufficiently secure. The use of PUFs is a viable option for mitigating these shortcomings. On the other hand, some solutions have been geared for applications of ad hoc networks. For example, Wang [16] proposed a bi-directional authentication scheme using elliptic curve encryption and bilinear pair mapping theory, which improves efficiency and security. In addition to the heavy computational load, this approach requires storing the device identity at the RSU. Patil et al. [17] presented a protocol that utilizes blockchain smart contracts to facilitate the authentication of an IoT

device by miners in the blockchain network. Yet, they employed the Diffie–Hellman key exchange protocol, which is computationally heavy. The AKAP-IoV system, proposed by Bojjagani et al. [18], enables mutual authentication and key management among various entities, including vehicles, roadside units, and fog and cloud servers. AKAP-IoV applies the elliptic curve integrated encryption scheme (ECIES) for encryption and decryption, as well as the elliptic curve digital signature algorithm (ECDSA) for signature generation and verification; neither ECIES nor ECDSA is lightweight. Similarly, Bagga et al. [19] proposed a Mutual Authentication and Key Management Scheme for an IoV-enabled Intelligent Transportation System, referred to as MAKMS-IoV. MAKMS-IoV employs elliptic curve cryptography (ECC) for two levels of authentication and session key agreement. The first level pertains to a cluster head in a vehicle cluster and its associated RSU. The second level pertains to authentication and session key agreement between any two neighboring vehicles in a cluster (V2V). However, these protocols introduce a significant computational load. Wallrabenstein [20] aims to reduce the computational complexity of the authentication process by employing only ECC. Nevertheless, this approach requires some alterations in the device hardware. It is worth noting that some work has focused on authenticating the shared data in IoV rather than the source of such data, i.e., the vehicle itself. For example, HIDE [21] factors in the spatial dependency of traffic data to assess the validity of the claimed mobility patterns of vehicles.

Some security solutions have exploited the advantages of PUFs. Chatterjee et al. [13] proposed an authentication protocol that utilizes PUF, along with identity-based encryption and a keyed hash function. The protocol of Yoon et al. [22] is also PUF based and seeks to establish mutual authentication among IoT devices. However, the protocol introduces additional complexity via the encryption of the exchanged CRPs between devices. Furthermore, the protocol requires the involvement of an intermediary server to store CRPs and generate secure keys. Additionally, Fakroon et al. [23] introduced a multi-factor authentication protocol that relies on PUFs and user passwords. Alladi and Chamola [24] aim to provide a secure authentication method for Healthcare IoT devices. The registration process involves storing the CRPs of the PUF in a database, making it vulnerable to machine learning attacks. Nimmy et al. [25] proposed an authentication protocol for IoT that leverages geometric threshold secret sharing and PUF. This protocol aims to eliminate the need for the explicit storage of CRPs in the verifier's database. However, the verifier is still required to store the share of the challenge and the hash of the response. Moreover, Jiang et al. [26] proposed a three-factor authentication protocol for IoV. Such a protocol is designed to provide secure communication between a pair of honest parties, namely, the vehicle sensor and the user, or the vehicle sensor and the data center. It utilizes ECC, hash functions, and PUFs as well as string concatenation and XOR operations. Yet, an attacker can potentially extract the shared session key between the two honest parties. All the aforementioned protection techniques require a secure server for authenticating the underlying network nodes.

Although a PUF is designed to be unclonable, it is still susceptible to modeling attacks. This happens when an attacker acquires a sufficient number of CRPs. For instance, the attacker could eavesdrop on a prover node to intercept the authentication messages exchanged with other nodes, i.e., verifiers. With the intercepted messages, the attacker can create a machine-learning model that behaves like the prover's PUF and can predict the responses for unused challenges. In order to address such a vulnerability, Majzoobi et al. [27] proposed to send only a subset of the response bits to the verifier instead of the entire set of bits. The subset of the response is determined using a synchronized random number generator between the prover and verifier. Another approach is presented by Ebrahimabadi et al. [28], where the challenge bit string undergoes a process of shuffling and is subsequently partitioned across multiple messages. Furthermore, challenge obfuscation has been explored as a technique in which the challenge bit strings are encrypted or hashed, and the encrypted version is then used to authenticate the nodes in the PUF [29].

P-MAP [30] is designed to provide mutual authentication and mitigate modeling attacks. It employs two challenges and a bitwise binary operation that is unique to the

communicating nodes. However, while this mechanism is effective at countering modeling attacks, it is important to note that P-MAP has limitations. Notably, an attacker may still be able to access the challenge bits, and the security of the protocol is dependent on the secrecy of the binary operation. The proposed protocol in this paper incorporates the advantageous features of MIMO technology to prevent adversaries from accessing challenge and response bits. This renders machine learning-based modeling attempts futile. The utilization of MIMO technology ensures that the adversary is effectively deprived of the requisite knowledge to undertake an attack on the system. Tang et al. [31] leveraged MIMO technology to ensure secure transmission between two nodes through the use of a "key bit" for encrypting confidential information. The key is encoded in the indexes of the activated/deactivated antenna combination of the receiver. The approach was subsequently extended in [32] to enable the sharing of a broadcast key with a group of devices. However, this method is vulnerable to impersonation attacks. To address such a security threat, our proposed approach incorporates PUFs.

3. System Model and Approach Overview

This section covers some preliminaries, highlights the underlying network operation, enumerates the made assumptions, and provides an overview of the proposed security solution.

3.1. Physical Unclonable Functions

The fundamental design basis of PUF is that there will always be small discrepancies in microelectronic circuits due to manufacturing imperfection [33]. Such imperfection is tolerated and does not significantly impact how efficiently integrated circuits operate. PUFs have been constructed to take advantage of these variations to produce a distinct hardware-driven fingerprint [33]. A PUF generates a unique mapping from an input bit string, referred to as a challenge, to an output bit that constitutes the PUF response. To clarify, Figure 2 shows the design of an Arbiter-PUF, which is one of the prominent PUF designs. The Arbiter-PUF is designed to exploit the variation in propagation delays. Since not every integrated circuit encounters the same delay, the latched value for the same challenge bits will vary and be influenced by the device manufacturing despite implementing the same circuit. Thus, for each challenge C, a response R is generated uniquely; the relationship between C and R is represented as $PUF(C) = R$. PUFs are categorized based on the size of the challenge bits as strong or weak. The fundamental classification is related to the number of combinations, i.e., 2^n. A strong PUF (large n) is favored for authentication, while a weak PUF latter is often viewed as suitable enough for key generation purposes.

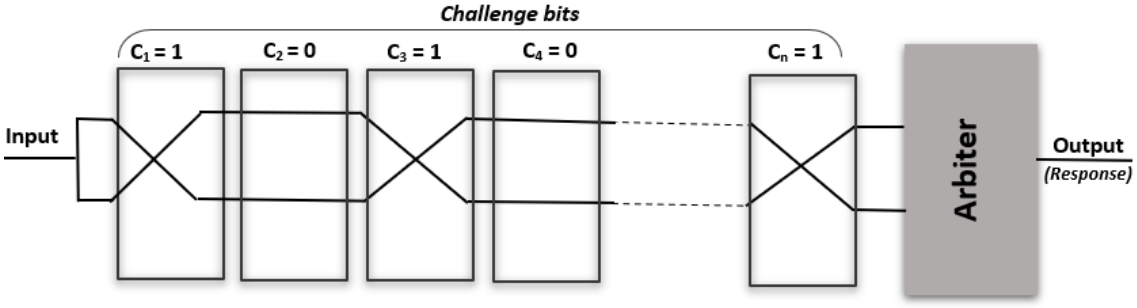


Figure 2. The structure of an n-bit Arbiter-PUF. Depending on the setting of an active switch (multiplexer) in each cell, every signal propagates through different paths within the cell. The challenge bits configure the cells and consequently define a distinct path and propagation delay. Therefore, the response of the Arbiter-PUF is generated based on the faster path of the two signals when the challenge bits are fed in.

3.2. System and Threat Models

The system model considered in this paper consists of a vehicle and an RSU as shown in Figure 1. Every node is equipped with a PUF, which is used for generating a response when queried with a challenge bit string. On a vehicle, the PUF could be embedded in the on-board computer. We assume that each node has a MIMO antenna array, which enhances the link quality while enabling more efficient use of the spectrum. The distance between each antenna array segment is greater than half a radio frequency wavelength. We denote the number of antennas of a vehicle δ_A and the RSU δ_B, by N_{δ_A} and N_{δ_B}, respectively. For medium access, standard time division multiplexing is employed. Since our proposed protocol essentially is geared for authentication, a large set of CRPS is required to counter brute-force attacks by an adversary. Thus, a strong PUF is incorporated to satisfy such a requirement. The presentation in the rest of the paper is based on the use of an Arbiter-PUF, discussed above. Nonetheless, the proposed authentication protocol can be applied to other strong PUF designs.

Although a PUF is deemed effective for authentication, it could be susceptible to modeling attacks, wherein an attacker obtains CRPs of the PUF and imitates the characteristics by building a machine-learning model. To clarify, the adversary intercepts the communication between two nodes, in our case a vehicle δ_A and one or more RSUs to capture a sufficient CRP count. The intercepted CRPs are then used to train a machine learning model for the PUF of δ_A. Such an attacker would then be able to predict the response of the vehicle's PUF, denoted by PUF_{δ_A}, to any assigned challenge bits. The attack scenario is represented in Figure 1, where a passive adversary δ_{Eve} with $N_{\delta_{Eve}}$ antennas is eavesdropping on the communication link between δ_A and δ_B. It is thus essential to protect the CRPs in order to safeguard against impersonation attacks.

3.3. Approach Overview

The objective of this paper is to establish a secure communication session between a vehicle δ_A and RSU δ_B by performing mutual authentication between these two nodes. Nonetheless, the proposed protocol can be applied for V2V as well. We introduce a lightweight protocol that enables mutual authentication between a vehicle and RSU by utilizing PUFs and a MIMO-based mapping technique to enhance communication security against the threat of device hacking. In our approach, vehicles can be authenticated without the need for a third party during network operation. However, a trusted third party might be needed in the enrollment phase. In the enrollment phase, the RSU will be provided a collection of CRPs derived from the PUF of the vehicles within the network. For example, the vehicle δ_A will share a set $\gamma_{B\to A}$ of CRPs with the RSU, where $|\gamma_{B\to A}|$ is not sufficient for developing an effective machine learning model of the PUF of δ_A.

To further enhance the security of communication, we employ a MIMO mapping technique to transmit a challenge bit pattern. Such a mapping determines the number of antennas utilized by the communicating nodes. The idea is to partition the challenge bits into $N_{\delta_A} - N_D$ segments, where N_{δ_A} is the number of the antennas that a vehicle has, and N_D is the number of deactivated antennas. The set of segments Seg is ordered, where the order is determined based on the node ID. For example, assume $N_{\delta_A} = 4$ and one antenna is deactivated, i.e., $N_D = 1$; generally, the number of deactivated antennas can take any value that is less than N_{δ_A}. A possible segmentation order for δ_A may be $Seg = \{s_2, s_3, s_1\}$; we note that another ordering can be pursued as long as it can be inferred based on the node ID. Then, the RSU δ_B will deactivate one of δ_A's antennas and activate the others. This process encodes an index that indicates which antenna holds a portion of C. The vehicle can use the same method to transmit the PUF response. The proposed protocol is discussed in detail in the next section.

4. Protocol Design

The proposed protocol has two phases, namely, enrollment and operation. The latter covers decoding at the receiver, challenge bits obfuscation using MIMO precoding at the sender, and physical layer channel estimation.

4.1. Enrollment Phase

During the enrollment process, each node needs to share specific information in order to become part of the network. Once enrolled, the newly joined vehicle will share a subset of the CRPs with the RSUs. To illustrate, if a vehicle δ_i shares Γ_i in the system, where Γ_i is a subset of all CRPs of the PUF of δ_i (denoted by PUF_i), after that, the RSU δ_j will have $\gamma_{i\to j}$ s.t. $\gamma_{i\to j} \subset \Gamma_i$. To ensure a sufficient variety of the provided CRPs of PUF_i within the RSUs in the system, γ will be distinct for each RSU s.t. $\gamma_{i\to j} \neq \gamma_{i\to g}$ for all $j \neq g$, where Γ_i is constructed based on the number of RSUs in the network. Additionally, each node (i.e., vehicle/RSU) will be provided with a segmentation order Seg_i for other nodes in the system. The proposed protocol utilizes the PUF incorporated in each device to identify the segmentation by defining $Seg_i = PUF_j(ID_i)$.

We note that the process of enrollment can be streamlined through the utilization of a trusted server, which would be particularly beneficial if nodes are joining the network at varying intervals. However, it is important to recognize that this approach remains distributed in nature, as the enrollment phase serves solely as an initialization process, and no centralized entity is involved during the operation phase. Once enrolled, the node will transition to the operation phase, wherein inter-node interaction is application dependent and will be further elucidated in subsequent subsections.

4.2. Channel Estimation

As illustrated in Figure 1, a vehicle attempts to communicate with an RSU node. We assumed that the communication link between the vehicle and the RSU could work for any frequency band. Due to weak non-line-of-sight (NLoS) links in the outdoor environment, the line-of-sight (LoS) link is the only channel we consider between the vehicle and the RSU. The gain between the antenna at the vehicle δ_A and the antenna at the RSU δ_B can be written as [34]:

$$h_{\delta_{A_i},\delta_{B_j}} = \frac{p_0}{d^2_{\delta_{A_i},\delta_{B_j}}} \tag{1}$$

where $d_{\delta_{A_i},\delta_{B_j}}$ is the distance between the i^{th} antenna at the vehicle to the j^{th} antenna at the RSU, with $2 \leq i \leq N_{\delta_A}$ and $2 \leq j \leq N_{\delta_B}$. Recall that N_{δ_A} and N_{δ_B} are the number of antennas that a vehicle and an RSU have, respectively. p_0 denotes the channel gain at a reference distance of 1 and is calculated as $p_0 = (\frac{\mathcal{L}}{4\pi f})^2$, where $\mathcal{L}$ is the speed of light, and f is the operating frequency. To apply our protocol, first δ_A sends a pilot signal to δ_B in a time that is lower than the channel coherence time [35]. δ_B estimates the up-link channel using:

$$\mathbf{H}_{\delta_A\delta_B} = \begin{pmatrix} h_{\delta_{A_1},\delta_{B_1}} & h_{\delta_{A_1},\delta_{B_j}} & \cdots & h_{\delta_{A_1},\delta_{B_{N_B}}} \\ \vdots & \vdots & \ddots & \vdots \\ h_{\delta_{A_{N_A}},\delta_{B_1}} & h_{\delta_{A_{N_B}},\delta_{B_j}} & \cdots & h_{\delta_{A_{N_A}},\delta_{B_{N_B}}} \end{pmatrix} \tag{2}$$

where $\mathbf{H}_{\delta_A\delta_B} \in M^{N_{\delta_A}\times N_{\delta_B}}$ reflects the engagement of all antennas of δ_A and δ_B, and M is a matrix with a size of $i \times j$. In order to obtain the corresponding down-link channel, δ_B transposes $\mathbf{H}_{\delta_A\delta_B}$ as $\mathbf{H}_{\delta_B\delta_A} = \mathbf{H}^T_{\delta_A\delta_B}$. The RSU will need to normalize the estimated channel

matrix to reduce the possible impact of path loss, then will compute the precoding weights space using zero-forcing precoding [36] $\mathcal{W} \in M^{N_{\delta_B} \times N_{\delta_A}}$ as:

$$\mathcal{W} = \frac{\mathbf{H}^H_{\delta_A\delta_B}(\mathbf{H}_{\delta_A\delta_B}\mathbf{H}^H_{\delta_A\delta_B})^{-1}}{\|\mathbf{H}^H_{\delta_A\delta_B}(\mathbf{H}_{\delta_A\delta_B}\mathbf{H}^H_{\delta_A\delta_B})^{-1}\|} = (w_1, w_2, ..., w_{N_{\delta_A}}) \tag{3}$$

where each column vector $w_j \in M^{N_{\delta_A} \times 1}, j = 1, 2, .., N_{\delta_B}$ is normalized as $\|w_j\|^2 = 1$. Thus

$$\mathbf{H}_{\delta_A\delta_B}\mathcal{W} = \text{diag}(\frac{1}{\|w_1\|}, \frac{1}{\|w_2\|}, ..., \frac{1}{\|w_{N_{\delta_A}}\|}) \tag{4}$$

4.3. Challenge Bits Mapping

Let $\mathbf{e}$ be the set of antenna indices, i.e., $\mathbf{e} = \{e_1, e_2, e_3, ..., e_{N_{\delta_A}}\}$. The cardinality of $\mathbf{e}$ depends on the number of antennas (N_{δ_A}) of δ_A. Our proposed protocol maps the challenge bit string C utilizing these antennae indices. Specifically, when δ_B intends to transmit the bit string C, it will activate a certain combination of the antenna elements of δ_A. An activated antenna index is represented by "1", while an inactivated index is represented by "0". Thus, we construct the non-zero precoding weights $\mathcal{W}(\mathbf{e})$ by excluding the zero column vector of $\mathcal{W}$ and combine the remaining ($N_{\delta_A - 1}$) column as:

$$\mathcal{W}(\mathbf{e}) = \sqrt{\frac{P_w}{N_{\delta_A} - 1}} \sum_{j=1}^{In(\mathbf{e})} w_j, \tag{5}$$

where P_w denotes the transmit power and $In(\mathbf{e})$ represents the index of non-zero antennas in $\mathbf{e}$. Based on (1), (2), and (5), the received signal by δ_A can thus be represented as:

$$\mathbf{Y}_{\delta_A} = \mathbf{H}_{\delta_B\delta_A}\mathcal{W}(\mathbf{e})C + n = \sqrt{P_s}\mathbf{H}_{\delta_B\delta_A} \sum_{j=1}^{(N_{\delta_A} - 1)} w_j C + n \tag{6}$$

where $n \in M^{N_{\delta_A} \times 1}$ is the additive Gaussian noise of the signal received by δ_A, and $\mathbf{Y}_{\delta_A} = (y_1, y_2, y_3, ..., y_{N_{\delta_A}}) \in M^{N_{\delta_A} \times 1}$ indicates the received signals vector. P_s is the transmit power on each transmission s.t. $P_s = \frac{P_w}{(N_{\delta_A} - 1)}$. Based on the activated\deactivated antenna elements, the received signal of δ_A s.t. $y \in \mathbf{Y}_{\delta_A}$ can be written as:

$$y_j = \frac{\sqrt{P_w}}{\|w_j\|}C + n, \qquad \text{(an active antenna)} \tag{7}$$

$$y_j = n, \qquad \text{(non-active antenna)} \tag{8}$$

From (5)–(8), the received signal of δ_A will be:

$$\mathbf{Y}_{\delta_A} = \sqrt{P_s}(\frac{1}{\|w_1\|}, ..., 0, ..., \frac{1}{\|w_{N_{\delta_A}}\|})^T C + n \tag{9}$$

where "0" in the position of the antenna implies it is inactive. To illustrate, assume that $N_{\delta_A} = 5$, and that the RSU δ_B sets $N_D = 1$ and disables, i.e., deactivates, the second antenna; hence, the antenna indices can be written as $\mathbf{e} = (10111)$. Then, δ_B transmits the challenge bits C in four segments s_1, s_2, s_3, and s_4 using the activated antennas. Effectively, C is constructed by combining the segments s_1, s_2, s_3, and s_4, where each segment reflects a subset of C, e.g., $s_1 = \{c_1, .., c_{16}\}, s_2 = \{c_{17}, .., c_{32}\}, s_3 = \{c_{33}, .., c_{48}\}, s_4 = \{c_{49}, .., c_{64}\}$. Assume that Seg_A is the segmentation order of δ_A, where $Seg_A = (s_3, s_2, s_1, s_4)$. The antenna index mapping will be $e_1 = s_2$, $e_3 = s_3$, $e_4 = s_1$ and $e_5 = s_4$. Because the second antenna is

not activated, it will not convey any part (bits) of C. Therefore, the eavesdropper has to recognize the segmentation of C, even if the antenna index $\mathbf{e}$ is exposed. As aforementioned, the node ID is used to infer the segmentation order for each node.

4.4. Decoding Transmitted Bits

At the final stage, once the vehicle receives the down-link signal, it will determine the indices of the deactivated antenna segments to correctly construct the challenge bit C. To achieve this, δ_A determines if the i^{th} antenna index is activated or not by utilizing the following function, which seeks the lowest signal-plus-noise (LSPN) value:

$$f_e(\mathbf{Y}_{\delta_A}) = \text{index}\left[\arg\min(|y_1|^2, |y_2|^2, ..., |y_{N_{\delta_A}}|^2)\right] = \hat{\mathbf{e}}(i) \tag{10}$$

Using $\hat{\mathbf{e}}$, δ_A identifies the antenna segments that are activated and cover C. These observed bits are then combined to form the complete challenge bits C. To clarify, let us consider the aforementioned example with $N_{\delta_A} = 5$, and $N_D = 1$. In such a case, $\hat{\mathbf{e}} = (1, 0, 1, 1, 1)$, where four challenge bits, namely, s_3, s_2, s_1, and s_4, will be individually received on antennas 0, 2, 3, and 4, respectively. Seg_A is then used to construct C such that $Seg_A(s_3, s_2, s_1, s_4) = C$. Subsequently, C is applied to PUF_A to generate R, where $PUF_A(C) = R$. Finally, δ_A transmits R by following the above steps. Upon receiving R, δ_B compares R with the value obtained during the enrollment phase. δ_A is authenticated upon a successful match. The message sequence during the operation phase of the proposed protocol is depicted in Figure 3.

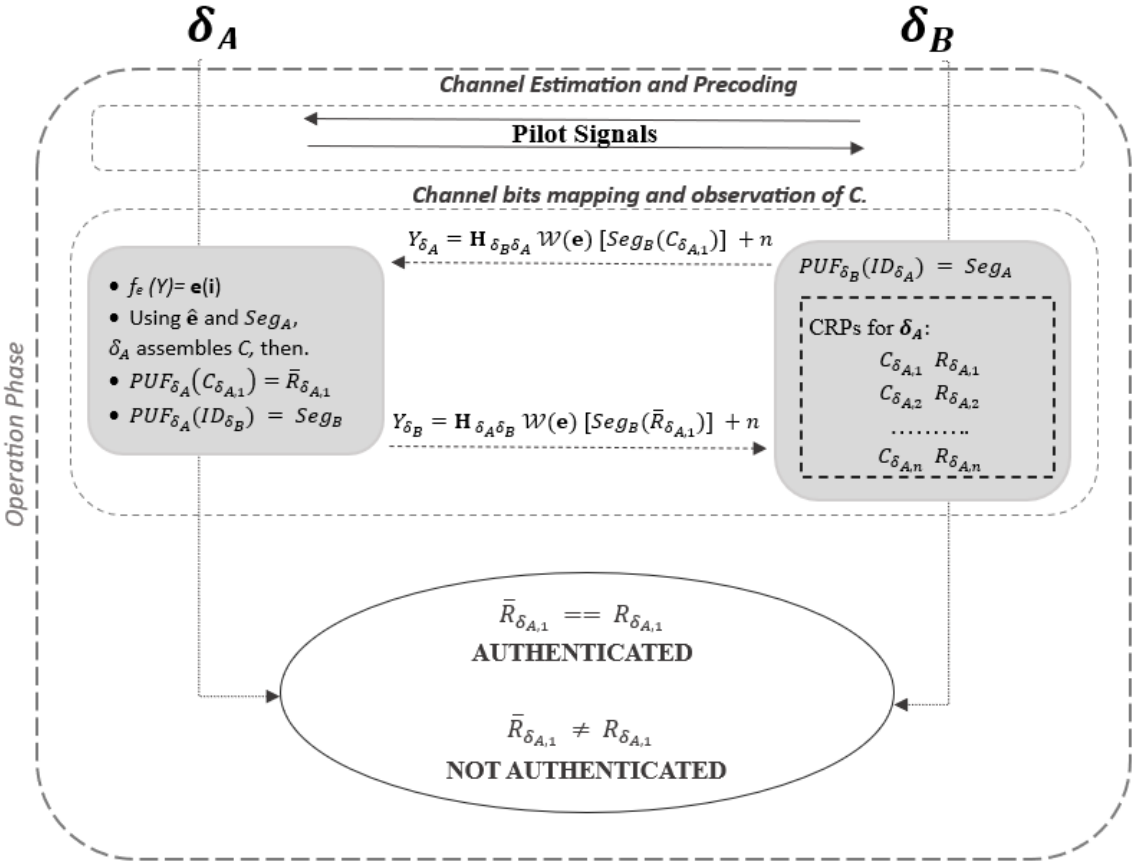


Figure 3. A sequence diagram to illustrate the message exchange between δ_A and δ_B.

5. Validation Setup

We implemented the Arbiter-PUF design described earlier in Figure 2 using MATLAB on PC with AMD Ryzen 7 5700U processor running Windows 10 with 16 GB memory. To assess the robustness of our PUF implementation, we considered the performance metrics described in Appendix A; the uniformity of the utilized Arbiter-PUF is 47%, with a uniqueness of 49.69%. As mentioned earlier, mitigating the noise effect caused by ambient temperatures is out of the scope of this work. In other words, the reliability of the PUF was evaluated under a normal temperature. Therefore, the hamming distance between the responses is 0. We further used MATLAB to simulate the IoV operation. The simulation parameters were consistent across all nodes, including vehicle, RSU, and the eavesdropper, all of which shared the same number of antennas, i.e., $N_{\delta_A} = N_{\delta_B} = N_{\delta_{Eve}} = 5$. Assuming that the vehicle is mobile, our authentication protocol is applied while the SNR varies from 0 dB to 30 dB based on the distance, transmitted power, and path loss between the two communicating nodes. It was assumed that white Gaussian noise had a zero mean. An SVM is utilized as a representative machine learning technique to model how an adversary δ_{Eve} might execute a cloning attack on the authentication protocol.

For the adversary to launch any cyberattacks, such as impersonation, data forgery, and man-in-the-middle attacks, the underlying device secrets need to be uncovered. In the context of PUFs, that means being able to model the challenge–response mapping through the incorporation of ML techniques. Recall that a key advantage of the PUF design is that it is tamper resistant, and the CRPs (device secrets) are not stored in memory. Hence, our analysis focused on thwarting modeling attacks. We initially used SVM and NN to model the Arbiter-PUF without the application of our approach. When using 5000 CRPs, SVM was able to achieve an accuracy of 99% and 98% for modeling the 16-bit and 64-bit PUF, respectively, as reported in Figure 4. We repeated the experiment using NN, which consisted of an input layer with 64 nodes for 64-bit PUF and 16 nodes for 16-bit PUF, and one hidden layer with 2 and 100 neurons for 16-bit and 64-bit, respectively. An output layer was added with a sigmoid activation function [37]. The first two layers utilized a rectified linear activation function (Relu) to achieve high performance. As shown in Figure 4, when using 5000 CRPs, NN could successfully model the 16-bit and 64-bit PUFs with 99% accuracy.

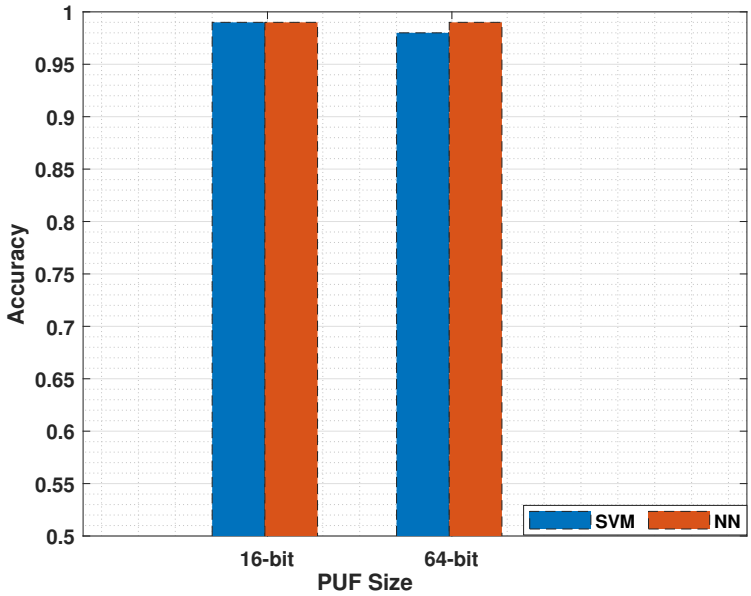


Figure 4. Accuracy of modeling 16-bit and 64-bit Arbiter-PUFs using SVM and NN.

6. Performance Results and Discussion

During the operation phase, an eavesdropper δ_{Eve} may intercept the communication between δ_A and δ_B with the intention to acquire a significant number of CRPs to mimic the δ_A PUF (PUF_A), thereby impersonating δ_A. The MIMO mapping technique in our proposed protocol hinders such an attacker from entirely recording the challenge bits C without being aware of $f_{\mathbf{e}}$ to obtain $\mathbf{e}$. We implemented three attack scenarios aimed at impersonating δ_A by modeling its PUF: (1) The attacker acts as a malicious node within the network with complete awareness of the authentication protocol. (2) Distinct from the previous case, here, the adversary lacks a detailed understanding of the protocol but is aware of the existence of an index mapping function ($f_{\mathbf{e}}$) without knowledge of how $f_{\mathbf{e}}$ is being applied. (3) The external attacker does not know the authentication protocol. The following discusses the results:

- High-awareness attack ($\delta_{Eve,1}$): In this case, $\delta_{Eve,1}$ obtains $\mathbf{e}$, which indicates whether the antenna is activated or not. The comparison of $\delta_{Eve,1}$ and δ_A in Figure 5 shows that $\delta_{Eve,1}$ finds $\mathbf{e}$ with a probability of 83% at the ideal SNR value 30 dB, while δ_A has 99%. Hence, the eavesdropper will record C as $\hat{C}$, as the RSU includes $Seg_A(C)$ in the request message rather than the actual challenge bit string C. This is emphasized by the probability distribution in Figure 6; such a figure shows the case when $\delta_{Eve,1}$ has knowledge of $Seg_A(C)$, where the x-axis presents the SNR values and y-axis shows the probability that the attacker correctly observes C with varying the updating period of CRPs. $\delta_{Eve,1}$ attempts to identify Seg_A; yet, the latter is changed periodically. Such analysis is consistent with the results in Figure 7, where the x-axis shows the recorded number of CRPs of PUF_A by δ_{Eve}, and the y-axis reflects the ML accuracy of modeling the PUF_{δ_A} with 10 dB SNR. Figure 7 demonstrates the modeling attack performed on two PUF sizes, 16-bit and 64-bit. As shown, the highest accuracy that the ML model can achieve is not greater than 54%, which is clearly a random guess, given the Boolean nature of the PUF response.
- Partial-awareness attack ($\delta_{Eve,2}$): In this type of attack, $\delta_{Eve,2}$ is aware of $f_{\mathbf{e}}$ but does not realize how it is being used. For example, let the antenna indices be $\mathbf{e} = (1110)$; one potential scenario by the adversary is dropping the first antenna index such that $\mathbf{e}_{Eve} = (0111)$. Thus, the probability of $\delta_{Eve,2}$ to successfully predict the antenna indices $\mathbf{e}$ for the target node δ_A can be expressed as $Pr[\mathbf{e} = \mathbf{e}_{Eve}] = \frac{1}{N_{\delta_A}}$. This is shown in Figure 5, where $\delta_{Eve,2}$ has the probability of 0.2. Such a modeling attack scenario will fail in building a ML model using the captured CRPs as shown in Figure 7, where the partial-awareness attack is simulated to model the PUF of δ_A considering two 16-bit and 64-bit PUFs.
- Non-awareness attack ($\delta_{Eve,3}$): This attacker does not have any knowledge about the protocol configuration. Thus, $\delta_{Eve,3}$ will expect that all antennas are active since he/she does not know about either $f_{\mathbf{e}}$ or $\mathbf{e}$. Consequently, $\delta_{Eve,3}$ will record the challenge bits as 20 bits, considering the PUF size as 16 bits. To illustrate, assume the challenge bits being sent are 16 bits and $N_{\delta_{Eve},3} = 5$. Since $\delta_{Eve,3}$ assumes all antennas are active, none of the antennas will be ignored. Thus, the total estimated bits would be 20 bits rather than 16 bits. Such a scenario is reflected in Figure 6, where the probability for $\delta_{Eve,3}$ is nearly 0.2. Accordingly, it is expected to find that the accuracy of $\delta_{Eve,3}$ in modeling the δ_A PUF is completely random as shown in Figure 7, where the highest accuracy achieved does not succeed 53% in both the 16-bit and 64-bit PUFs.

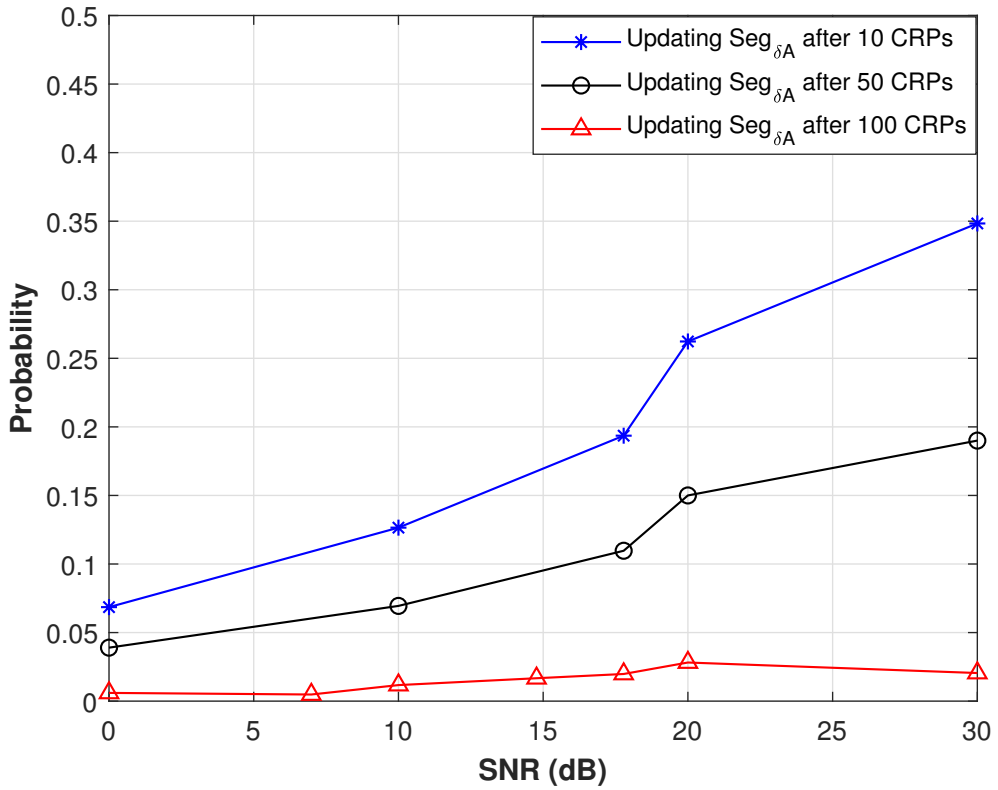


Figure 5. The probability of observing **e** correctly by $\delta_{Eve,1}$.

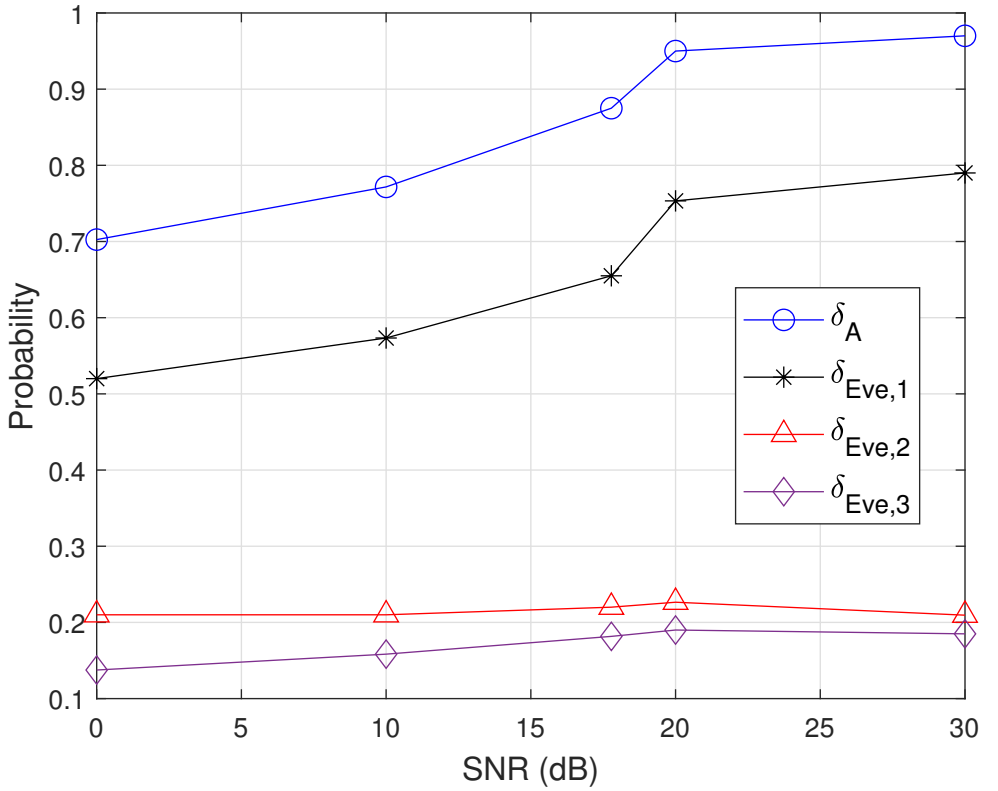
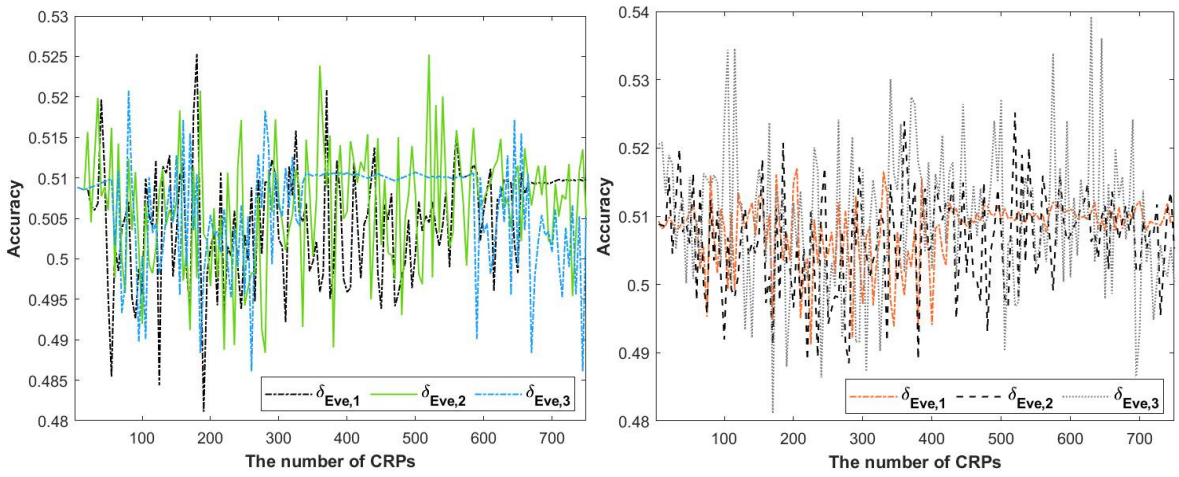


Figure 6. The probability of accurately observing C.



(**a**) 16-bit PUF (**b**) 64-bit PUF

Figure 7. Our proposed protocol's accuracy in modeling 16-bit and 64-bit Arbiter-PUF implementations using SVM.

7. Approach Robustness

To demonstrate the practicality of the proposed approach, we analyze the error rate using two measurement parameters—the Probability of the Error Index (PEI) and the Probability of the Error Challenge (PEC)—as follows:

- PEI: This is the probability of the error index $\hat{e}$ being experienced by a node and can be expressed as:

$$PEI = Pr[e(\hat{i}) \neq e(i)] \tag{11}$$

PEI can be calculated mathematically using:

$$PEI = 1 - Pr\left[\min(|y_1|^2, |y_2|^2, ..., |y_{N_{\delta_A}}|^2)\right] \geq |y_{e(\hat{i})}|^2 \tag{12}$$

where $|y_{e(\hat{i})}|$ is the received signal at the non-activated antenna.

- PEC: This reflects the probability of an erroneous challenge $\hat{C}$ being extracted by the receiver. PEC can be expressed as:

$$PEC = Pr[\hat{C} \neq C] \tag{13}$$

The relationship between PEI and PEC can be expressed as:

$$PEC \simeq 1 - \left[1 - P_{PEI}\right]^{N_{Seg}(\delta_A)} \tag{14}$$

where $N_{Seg}(\delta_A)$ is the number of segments of the challenge bit string.

As demonstrated by the results in Figure 8, the segmentation mechanism in our approach has a very low error rate in extracting the challenge bits by the legitimate node (i.e., RSU δ_A). These results reflect an attacker who is fully aware of the approach, i.e., $\delta_{Eve,1}$, where the number of segments for δ_A varies from 2 to 32. For the largest segment count, only an error rate of 0.003 is experienced under 30dB SNR. Such a percentage has no notable effect on receiving the challenge bits correctly by δ_A. Thus, there is no advantage of knowing $N_{Seg}(\delta_A)$ since it is interpreted based on the node ID, and it changes periodically. This analysis concludes that having full knowledge of the operation and configuration of the proposed protocol will not allow the attacker to successfully model the PUF.

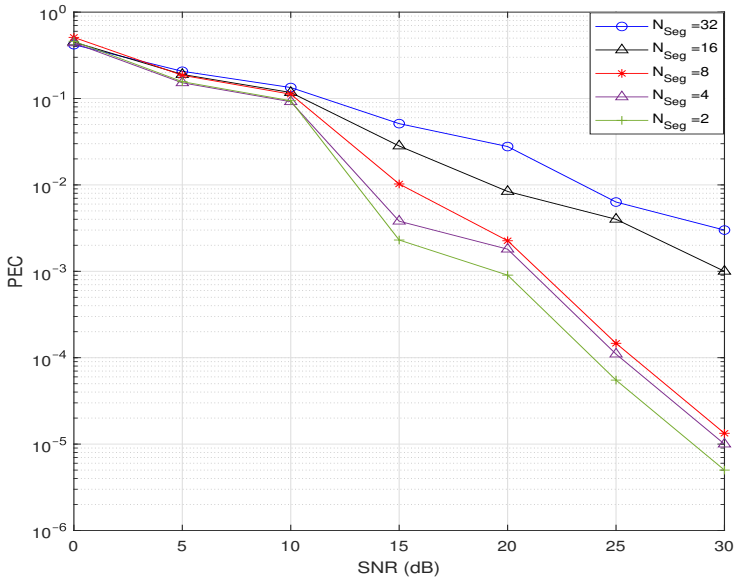


Figure 8. The impact of varying the size of *Seg* on *PEC*.

Figure 9 compares our protocol with the schemes of [32,38] in terms of PEC. As indicated by the results shown in Figure 9, our approach is as robust as the competing schemes, yet the challenge extracted by our approach reflects an obfuscated challenge and response transmissions. In [32,38], the secret information might be leaked, as both approaches entirely depend on their encoding techniques. However, the proposed protocol applies a node-specific function, where a PUF challenge C is partitioned into multiple segments while maintaining a very low PEC at the receiver side. As can be seen in Figure 8, with the highest number of segments, the receiver δ_A can only observe the challenge bits with a PEC of 0.003 at 30 dB. Thus, our protocol is more secure against modeling attacks since the exchanged CRPs are obfuscated using the aforementioned techniques. In addition, we consider the case where a user node δ_B and a vehicle δ_A pursue distributed authentication, which was not considered neither in [32] nor in [38].

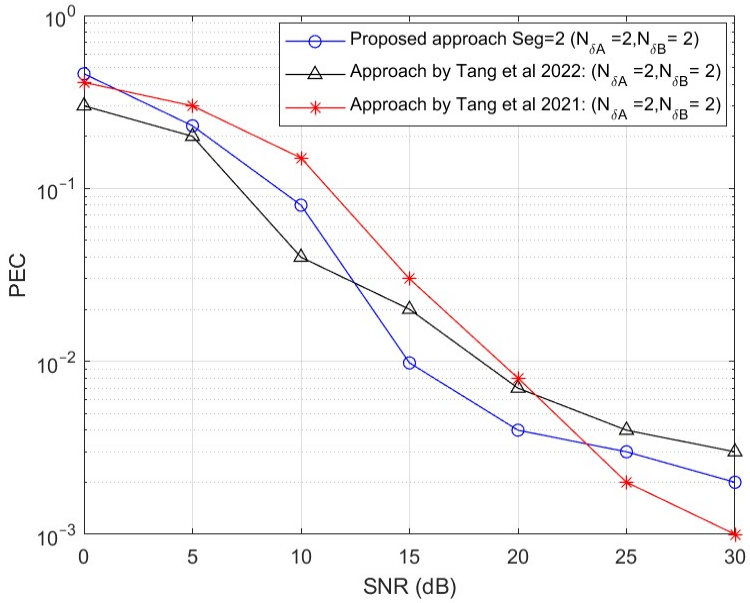


Figure 9. PEC comparison of the proposed approach with the approach in [32,38].

The probability that $\delta_{Eve,1}$ accurately observes both C and R simultaneously is:

$$Pr(\widehat{CRP} = CRP) = Pr(\hat{C} = C).Pr(\hat{R} = R \mid \hat{C} = C) \tag{15}$$

where $\widehat{CRP}$ denotes the successful inference of CRPs by $\delta_{Eve,1}$, whereas $\hat{C}$ and $\hat{R}$ indicate the observed values of C and R by $\delta_{Eve,1}$, respectively. Given the results in Figure 6, the maximum probability that $\delta_{Eve,1}$ correctly observes C is 0.8 and occurs when the SNR is set to 30 dB. Thus, even with a 0.8 probability of successfully guessing R, i.e., $Pr(\hat{R} = R) = 0.8$, according to Equation (15), the PUF modeling accuracy would not exceed 65%, which is quite low. Therefore, our approach is resilient against PUF modeling attacks.

The expression $PEI = Pr[e(\hat{i}) \neq e(i)]$ in (11) denotes that the non-activated antenna's observed index does not correspond to the desired non-activated antenna at δ_A. The value of PEI is intricately related to the parameters N_{δ_A}, N_{δ_B}, and P_w as reflected in Figure 8. Assuming that the background noise follows a zero and covariance one complex Gaussian distribution $\mathcal{CN}(0, \sigma^2_{\delta_B})$, Equation (12) indicates that when the j^{th} antenna is not activated, δ_B will detect an erroneous index if the minimum LSPN of the other $N_{\delta_B} - 1$ activated antennas exceeds that of such an inactive antenna (i.e., the j^{th} antenna). Theorem 1 below proves that achieving $PEI \to 0$ is always possible.

Theorem 1. *For any* $N_{\delta_A}, N_{\delta_B}, \leq \infty$, *when* $\frac{P_w}{\sigma^2_{\delta_B}} \to \infty$, $PEI \to 0$.

Proof. From (7) and (8),when SNR $\frac{P_w}{\sigma^2_{\delta_B}} \to \infty$

$$|y_x|^2 = [\lim_{\frac{P_w}{\sigma^2_{\delta_B}} \to \infty} |\frac{\sqrt{P_w}}{\|w_x\|}c + n_x|^2 \to \infty] \gg \lim_{\frac{P_w}{\sigma^2_{\delta_B}} \to \infty} |y_z|^2 = |n_z|^2 \forall x \in \boldsymbol{Ind}(e), \forall z \notin \boldsymbol{Ind}(e) \tag{16}$$

where ***Ind*** indicates the activated antenna indices. Consequently,

$$\lim_{\frac{P_w}{\sigma^2_{\delta_B}} \to \infty} Pr(|y_x|^2 > |y_z|^2) \to 1, \forall x \in \boldsymbol{Ind}(e), \forall z \notin \boldsymbol{Ind}(e) \tag{17}$$

From (17) and (11), Theorem 1 is proven. □

8. Conclusions

In the context of IoV, secure communication among vehicles and roadside units plays a pivotal role in preventing unauthorized access to sensitive information and the injection of malicious data. To support such a role, this paper presented a novel authentication protocol that utilizes hardware-based security primitives, namely PUFs. The proposed protocol allows vehicles and roadside units to authenticate each other. To prevent eavesdropping and impersonation, our protocol obfuscates the exchanged CRPs (challenge–response pairs) using the MIMO encoding technique. The paper also examines the resilience of the proposed approach against modeling attack capabilities for predicting the CRPs of the PUF. As a baseline, a machine learning attack using SVM and NN was applied and showed to achieve at least 98% accuracy when no protection is provisioned. When applying the proposed protocol, the CRP prediction accuracy did not exceed 54%, which indicates that it is similar to random guessing. In the future, we plan to examine the performance of our protocol using a prototype IoV.

Author Contributions: Conceptualization, M.A., A.A. and M.Y.; methodology, software, validation, data curation, writing—original draft preparation, visualization, and investigation M.A. and A.A.; formal analysis, resources, and writing—review, M.A., A.A. and M.Y.; supervision, and project administration, M.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

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

Notation

δ_A, δ_B, δ_{Eve}	Vehicle, RSU, and the eavesdropper *Eve*
N_{δ_A}, N_{δ_B}, $N_{\delta_{Eve}}$	The number of antennas for δ_A,δ_B, and δ_{Eve}
C, c	PUF challenge bits, where $c \in C$
R, r	PUF response bits, where $r \in R$
Γ_i	CRPs set for node i
$\gamma_{i \to j}$	A subset of CRPs for i to j, where $\gamma_i \in \Gamma_i$
Seg, s	A set of ordered segments of the PUF challenge C, where $s \in Seg$
$N_{Seg}(\delta_A)$	The segments counts of the challenge bit string for δ_A
N_D	The number of deactivated antennas
$\mathcal{W}$	Precoding weights space
$\mathbf{e}$, e	Antenna indices, where $e \in \mathbf{e}$
$\hat{\mathbf{e}}$	Antenna indices observed by δ_A
$\mathbf{Y}_{\delta_A}$	The received signal by node δ_A
p_0	Channel gain at a reference distance of 1
$d_{\delta_{A_i},\delta_{B_j}}$	Distance between ith antenna at δ_A and the jth antenna of δ_B
$\mathcal{L}$	The speed of light
P_w	Transmit power
P_s	Transmit power on each transmission
$\mathbf{H}_{\delta_A\delta_B}$	The engagement of all antennas of δ_A and δ_B
M	A matrix with size of $i \times j$
$In(\mathbf{e})$	The index of non-zero antenna in $\mathbf{e}$
$f_e()$	Function to determine active\inactive antennas

Appendix A. Evaluation Metrics of PUFs

In this section, we introduce two metrics, namely uniqueness and reliability, to evaluate the PUF design quality. Prior to proceeding with the computation of those metrics, it is necessary to expound on the fundamental concepts of Hamming distance and Hamming weight, which serve as the cornerstone for the metrics [39].

- Hamming Distance: The Hamming distance, which is a measure of the dissimilarity between two words, is defined as the number of positions where they vary. Specifically, for two words $x = (x_j)$ and $y = (y_j)$ of length n, the Hamming distance $d(x, y)$ is the count of all indices (j) such that x_j and y_j are not equal.
- Hamming Weight: The Hamming weight is used to measure the similarity between two words of equal length. A word is a sequence of symbols such as numbers, letters, or binary digits. The Hamming weight of a word is defined as the number of symbols that differ from a reference word, which is the zero vector denoted as 00...0. For a given word $x = x_1, x_2, x_3, ..., x_n$, the Hamming weight $HW(x)$ is the number of symbols $x_i \neq 0$ in x. This means that if a symbol in the word has a non-zero value, it is counted towards the Hamming weight calculation.

Appendix A.1. Uniqueness

PUF uniqueness refers to the ability of a single PUF instance to be uniquely identified from a group of comparable PUFs. The ideal value for uniqueness is 50%. To evaluate the performance of uniqueness, the Hamming distance (HD) is employed and is commonly referred to as "$Inter - chip\ HD$" [39]. For two chips x and y ($x \neq y$) possessing n-bit responses $R_x(n)$ and $R_y(n)$, respectively, for a specific challenge C, the average inter-chip HD among m chips can be defined as:

$$HD_{INTER} = \frac{2}{m(m-1)} \sum_{x=1}^{m-1} \sum_{y=x+1}^{m} \frac{HD(R_x(n), R_y(n))}{n} \times 100\% \quad \text{(A1)}$$

Appendix A.2. Reliability

The reliability of a PUF refers to how consistently it provides the same response to a given challenge across varying operating conditions, such as changes in temperature or voltage supply fluctuations. To evaluate the reliability of a PUF, the HD described above is used. This evaluation metric is called the $Intra-chip\ HD$ because it compares the response of a single chip, denoted as j, to a challenge input at normal operating conditions, with the same chip's response to the same input under varying conditions, such as different ambient temperatures or voltage supply fluctuations. Specifically, the n-bit reference response $R_j(n)$ is obtained from the chip j at normal operating conditions, while the same n-bit response $R'_j(n)$ is obtained under different conditions for the same challenge input [39]. Finally, the average $intra-chip\ HD$ for m samples/chips is calculated by taking into account the HD of each pair of responses obtained from a single chip under varying conditions, which can be defined as:

$$HD_{INTRA} = \frac{1}{m} \sum_{j=1}^{m} \frac{HD(R_j(n), R_j(n))}{n} \times 100\% \quad \text{(A2)}$$

From (A2), the PUF reliability can be written as:

$$Reliability = 100\% - HD_{INTRA} \quad \text{(A3)}$$

Appendix A.3. Uniformity

This metric quantifies the level of unpredictability in the responses produced by a PUF. It is determined by the proportion of 0s and 1s present in the PUF response bits. In the case of a completely random response, this proportion is 50%. The metric can be computed by determining the average Hamming weight of the responses as follows [40]:

$$Uniformity = \frac{1}{m} \sum_{j=1}^{m} r_j \times 100\% \quad \text{(A4)}$$

where m represents the total number of responses, and r_j is the Hamming weight of the jth response.

References

1. Yan, C.; Xu, W.; Liu, J. Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. *Def Con* **2016**, *24*, 109.
2. Duan, W.; Gu, J.; Wen, M.; Zhang, G.; Ji, Y.; Mumtaz, S. Emerging Technologies for 5G-IoV Networks: Applications, Trends and Opportunities. *IEEE Netw.* **2020**, *34*, 283–289. [CrossRef]
3. Dureja, A.; Sangwan, S. A Review: Efficient Transportation—Future Aspects of IoV. In Proceedings of the Evolving Technologies for Computing, Communication and Smart World, Singapore, 26 November 2020; pp. 97–108.
4. Goasduff, L. Gartner Predicts Outdoor Surveillance Cameras Will Be Largest Market for 5G Internet of Things Solutions over Next Three Years. 2019. Available online: https://www.gartner.com/en/newsroom/press-releases/2019-10-17-gartner-predicts-outdoor-surveillance-cameras-will-be#:~:text=Outdoor%20surveillance%20cameras%20will%20be%20the%20largest%20market%20for%205G,by%20the%20end%20of%202023 (accessed on 24 October 2023)
5. Maeng, S.J.; Yapıcı, Y.; Güvenç, İ.; Bhuyan, A.; Dai, H. Precoder design for physical-layer security and authentication in massive MIMO UAV communications. *IEEE Trans. Veh. Technol.* **2022**, *71*, 2949–2964. [CrossRef]
6. Garg, A.; Chauhan, A.; Shambharkar, P.G. Security Threats & Attacks in IoV Environment: Open Research Issues and Challenges. In Proceedings of the 2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT), Kannur, India, 11–12 August 2022; pp. 803–810. [CrossRef]

7. These Chinese Hackers Tricked Tesla's Autopilot into Suddenly Switching Lanes. 2019. Available online: https://www.cnbc.com/2019/04/03/chinese-hackers-tricked-teslas-autopilot-into-switching-lanes.html#:~:text=The%20group%20of%20cybersecurity%20researchers,where%20oncoming%20traffic%20would%20be (accessed on 24 October 2023)
8. Alladi, T.; Bansal, G.; Chamola, V.; Guizani, M. SecAuthUAV: A novel authentication scheme for UAV-ground station and UAV-UAV communication. *IEEE Trans. Veh. Technol.* **2020**, *69*, 15068–15077. [CrossRef]
9. Fotouhi, A.; Qiang, H.; Ding, M.; Hassan, M.; Giordano, L.G.; Garcia-Rodriguez, A.; Yuan, J. Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3417–3442.
10. Lounis, K.; Zulkernine, M. Lessons Learned: Analysis of PUF-Based Authentication Protocols for IoT. *ACM Digit. Threat.* **2022**, *4*, 1–33. [CrossRef]
11. Shamsoshoara, A.; Korenda, A.; Afghah, F.; Zeadally, S. A survey on physical unclonable function (PUF)-based security solutions for Internet of Things. *Comput. Netw.* **2020**, *183*, 107593.
12. Mall, P.; Amin, R.; Das, A.K.; Leung, M.T.; Choo, K.K.R. PUF-based authentication and key agreement protocols for IoT, WSNs, and Smart Grids: A comprehensive survey. *IEEE Internet Things J.* **2022**, *9*, 8205–8228. [CrossRef]
13. Chatterjee, U.; Govindan, V.; Sadhukhan, R.; Mukhopadhyay, D.; Chakraborty, R.S.; Mahata, D.; Prabhu, M.M. Building PUF based authentication and key exchange protocol for IoT without explicit CRPs in verifier database. *IEEE Trans. Dependable Secur. Comput.* **2018**, *16*, 424–437. [CrossRef]
14. Alkanhal, M.; Alali, A.; Younis, M. PUF-Based Authentication Protocol with Physical Layer-Based Obfuscated Challenge-Response Pair. In Proceedings of the ICC 2023—IEEE International Conference on Communications, Rome, Italy, 28 May–1 June 2023; pp. 5867–5872. [CrossRef]
15. Román-Castro, R.; López, J.; Gritzalis, S. Evolution and trends in IoT security. *Computer* **2018**, *51*, 16–25. [CrossRef]
16. Wang, C.; Dai, Z.; Zhao, D.; Wang, F. A Novel Identity-based Authentication Scheme for IoV Security. *Int. J. Netw. Secur.* **2020**, *22*, 627–637.
17. Patil, A.S.; Hamza, R.; Hassan, A.; Jiang, N.; Yan, H.; Li, J. Efficient privacy-preserving authentication protocol using PUFs with blockchain smart contracts. *Comput. Secur.* **2020**, *97*, 101958. [CrossRef]
18. Bojjagani, S.; Reddy, Y.C.A.P.; Anuradha, T.; Rao, P.V.V.; Reddy, B.R.; Khan, M.K. Secure Authentication and Key Management Protocol for Deployment of Internet of Vehicles (IoV) Concerning Intelligent Transport Systems. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 24698–24713. [CrossRef]
19. Bagga, P.; Das, A.K.; Wazid, M.; Rodrigues, J.J.P.C.; Choo, K.K.R.; Park, Y. On the Design of Mutual Authentication and Key Agreement Protocol in Internet of Vehicles-Enabled Intelligent Transportation System. *IEEE Trans. Veh. Technol.* **2021**, *70*, 1736–1751. [CrossRef]
20. Wallrabenstein, J.R. Practical and secure IoT device authentication using physical unclonable functions. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 22–24 August 2016; pp. 99–106.
21. Iranmanesh, S.; Abkenar, F.S.; Jamalipour, A.; Raad, R. A Heuristic Distributed Scheme to Detect Falsification of Mobility Patterns in Internet of Vehicles. *IEEE Internet Things J.* **2022**, *9*, 719–727. [CrossRef]
22. Yoon, S.; Kim, B.; Kang, Y.; Choi, D. Puf-based authentication scheme for iot devices. In Proceedings of the 2020 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Republic of Korea, 21–23 October 2020; pp. 1792–1794.
23. Fakroon, M.; Gebali, F.; Mamun, M. Multifactor authentication scheme using physically unclonable functions. *Internet Things* **2021**, *13*, 100343. [CrossRef]
24. Alladi, T.; Chamola, V.; Naren. HARCI: A two-way authentication protocol for three entity healthcare IoT networks. *IEEE J. Sel. Areas Commun.* **2020**, *39*, 361–369. [CrossRef]
25. Nimmy, K.; Sankaran, S.; Achuthan, K. A novel lightweight PUF based authentication protocol for IoT without explicit CRPs in verifier database. *J. Ambient Intell. Humaniz. Comput.* **2023**, *14*, 6227–6242. [CrossRef]
26. Jiang, Q.; Zhang, X.; Zhang, N.; Tian, Y.; Ma, X.; Ma, J. Three-factor authentication protocol using physical unclonable function for IoV. *Comput. Commun.* **2021**, *173*, 45–55. [CrossRef]
27. Majzoobi, M.; Rostami, M.; Koushanfar, F.; Wallach, D.S.; Devadas, S. Slender PUF protocol: A lightweight, robust, and secure authentication by substring matching. In Proceedings of the 2012 IEEE Symposium on Security and Privacy Workshops, San Francisco, CA, USA, 24–25 May 2012; pp. 33–44.
28. Ebrahimabadi, M.; Younis, M.; Karimi, N. A PUF-based modeling-attack resilient authentication protocol for IoT devices. *IEEE Internet Things J.* **2021**, *9*, 3684–3703. [CrossRef]
29. Farha, F.; Ning, H.; Ali, K.; Chen, L.; Nugent, C. SRAM-PUF-based entities authentication scheme for resource-constrained IoT devices. *IEEE Internet Things J.* **2020**, *8*, 5904–5913. [CrossRef]
30. Alkanhal, M.; Younis, M. P-MAP: PUF-based Mutual Authentication Protocol. In Proceedings of the ICC 2022—IEEE International Conference on Communications, Seoul, Republic of Korea, 16–20 May 2022; pp. 3424–3429.
31. Tang, J.; Jiao, L.; Zeng, K.; Wen, H.; Qin, K.Y. Physical layer secure MIMO communications against eavesdroppers with arbitrary number of antennas. *IEEE Trans. Inf. Forensics Secur.* **2020**, *16*, 466–481. [CrossRef]

32. Tang, J.; Wen, H.; Song, H.H.; Jiao, L.; Zeng, K. Sharing secrets via wireless broadcasting: A new efficient physical layer group secret key generation for multiple IoT devices. *IEEE Internet Things J.* **2022**, *9*, 15228–15239. [CrossRef]
33. McGrath, T.; Bagci, I.E.; Wang, Z.M.; Roedig, U.; Young, R.J. A puf taxonomy. *Appl. Phys. Rev.* **2019**, *6*, 011303. [CrossRef]
34. Alali, A.; Rawat, D.B.; Liu, C. Trajectory and power optimization in sub-THz band for UAV communications. In Proceedings of the ICC 2022—IEEE International Conference on Communications, Seoul, Republic of Korea, 16–20 May 2022; pp. 1–6.
35. Lao, Y.; Yuan, B.; Kim, C.H.; Parhi, K.K. Reliable PUF-based local authentication with self-correction. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **2016**, *36*, 201–213. [CrossRef]
36. Wong, K.K.; Pan, Z. Array gain and diversity order of multiuser MISO antenna systems. *Int. J. Wirel. Inf. Netw.* **2008**, *15*, 82–89. [CrossRef]
37. Santikellur, P.; Bhattacharyay, A.; Chakraborty, R.S. Deep learning based model building attacks on arbiter PUF compositions. *Cryptol. Eprint Arch.* **2019**, 566–573. Available online: https://eprint.iacr.org/2019/566 (accessed on 24 October 2023).
38. Tang, J.; Wang, R.; Song, H.H.; Wen, H. Fast and Efficient Physical Layer Secret Key Generation over Static Wireless Channels. In Proceedings of the 2021 7th ICCC, Chengdu, China, 10–13 December 2021; pp. 251–256. [CrossRef]
39. Halak, B. *Physically Unclonable Functions*; Springer: Berlin, Germany, 2018.
40. Maiti, A.; Gunreddy, V.; Schaumont, P. A systematic method to evaluate and compare the performance of physical unclonable functions. In *Embedded Systems Design with FPGAs*; Springer: New York, NY, USA, 2013; pp. 245–267.