

Article

Physical Unclonable Function Based Privacy-Preserving Authentication Scheme for Autonomous Vehicles Using Hardware Acceleration

Rabeea Fatima ¹, Ujunwa Madububambachu ¹, Ahmed Sherif ^{1,*} , Muhammad Hataba ², Nick Rahimi ¹ and Kasem Khalil ^{3,4} 

¹ School of Computing Sciences and Computer Engineering, University of Southern Mississippi, Hattiesburg, MS 39406, USA; rabeea.fatima@usm.edu (R.F.); ujunwa.madububambachu@usm.edu (U.M.); nick.rahimi@usm.edu (N.R.)

² Department of Computers and Systems, National Telecommunication Institute (NTI), Cairo 11768, Egypt; muhammad.hataba@nti.sci.eg

³ Electrical and Computer Engineering Department, University of Mississippi, Oxford, MS 38677, USA; kmkhalil@olemiss.edu

⁴ Department of Electrical Engineering, Assiut University, Assiut 71515, Egypt

* Correspondence: ahmed.sherif@usm.edu

Abstract

With the rise of smart cities, technology has enabled more efficient urban management. A key part of this is the Internet of Vehicles (IoVs), which connects vehicles to smart city systems to improve transportation safety and efficiency. This integrated system enables wireless connection between vehicles, allowing for the sharing of essential traffic information. However, with all this connectivity, there are growing concerns about IoV security and privacy. This paper presents a new privacy-preserving authentication scheme for Autonomous Vehicles (AVs) in the IoV field using physical unclonable functions (PUFs). This scheme employs a bilinear pairing-based encryption technique that supports search over encrypted data. The primary aim of this scheme is to authenticate AVs inside the IoV architecture. A novel PUF design generates random keys for our authentication technique, hence boosting security. This dual-layer security strategy safeguards against a range of cyber threats, including identity fraud, man-in-the-middle attacks, and unauthorized access to personal user data. The PUF design will guarantee the true randomness of the AVs' users' secret keys. To handle the large amount of data involved, we use hardware acceleration with different Field-Programmable Gate Arrays (FPGAs). Our examination of privacy and security demonstrates the achievement of the defined design goals. The proposed authentication framework was fully implemented and validated on FPGA platforms to demonstrate its hardware feasibility and efficiency. The integrated heterogeneous PUF achieves an average reliability exceeding 98.5% across a wide temperature range, while maintaining near-ideal randomness with an average Hamming weight of 49.7% over multiple challenge sets. Furthermore, the uniqueness metric approaches 49.9%, confirming strong inter-device distinguishability among different PUF instances. The complete authentication architecture was synthesized on Nexys-100T, Zynq-104, and Kintex-116 devices, where the design utilizes less than 80% of slice Look-Up Tables (LUTs), under 27% of on-chip memory resources, and below 16% of DSP blocks, demonstrating low hardware overhead.

Keywords: physical unclonable function; authentication; autonomous vehicles (AVs); hardware acceleration



Academic Editor: Ilsun You

Received: 29 December 2025

Revised: 2 February 2026

Accepted: 5 February 2026

Published: 7 February 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and

conditions of the [Creative Commons](https://creativecommons.org/licenses/by/4.0/)

[Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

In recent years, smart cities have undergone a massive transformation due to advancements in information and communication technologies. The Internet of Vehicles (IoVs) facilitates the collection of real-time traffic data, the control of traffic signals, and the effective distribution of traffic information, enabling the estimation of road network capacity and travel times. By processing data from IoVs, it becomes possible to improve traffic flow and ensure safe travel [1]. The transmission and management of data in the IoVs rely heavily on wireless channels, making them susceptible to threats such as information leakage and data attacks [2–4]. Ensuring the privacy and security of this continuously exchanged data, especially in authentication processes, is essential for maintaining system integrity and protecting user privacy in the IoVs ecosystem [5–11].

The increased connectivity and data interchange among vehicles cause privacy and security difficulties, which in turn pose a challenge to authentication in the IoV. Ensuring authenticity is crucial to preserving the integrity of the IoV ecosystem and protecting individual privacy, especially when wireless connectivity between vehicles increases the risk of unauthorized access and malicious data attacks. In addition, several drawbacks exist in current privacy-centric authentication frameworks for the IoV. One of these shortcomings is their vulnerability to attacks like identity fraud and data manipulation. Unfortunately, the majority of existing solutions are inadequate; they either struggle with scalability or require excessive processing resources to be feasible. The open and ever-changing nature of IoV networks may also be too much for existing solutions to manage, leaving users vulnerable to insufficient privacy protections [12–17].

In order to address these restrictions, we have developed a hardware-accelerated privacy-preserving authentication mechanism for the IoV that uses PUFs, a search-over-encrypted-data feature, and a bilinear-pairing-based encryption method. To guarantee the safe and precise transfer of vehicle data, this framework emphasizes privacy-preserving authentication. By including PUFs into key generation, an additional security layer is created, which enhances the privacy and security of IoV networks by utilizing distinct physical characteristics. This paper introduces a searchable symmetric-key encryption scheme that is suitable for both single-traffic management (like in a transportation department) and multi-user scenarios involving autonomous vehicles (AVs) in an IoV framework. In these scenarios, data, including AV identification information, is transmitted from both the traffic management system and the AVs themselves. Our authentication protocol enables the TMC and each AV to employ a single key to simultaneously encrypt AV identity data vectors (identifying vectors for all AVs overseen by a specific TMC, along with authentication requests from the AVs), while enhancing the server's capacity to match the encrypted vectors.

A Physical Unclonable Function (PUF) is a hardware security primitive that exploits inherent manufacturing process variations to generate unique and device-specific responses to given challenges [18–22]. Due to uncontrollable and random physical variations introduced during fabrication, each PUF instance exhibits distinct behavior that is extremely difficult to replicate or predict, even by the original manufacturer [23–25]. PUFs are commonly used for lightweight key generation, device authentication, and secure identification without storing secret keys in non-volatile memory, thereby reducing vulnerability to physical and side-channel attacks. Depending on the underlying entropy source, PUFs can be broadly categorized into delay-based, memory-based (e.g., SRAM PUFs), and oscillator-based PUFs, each offering different trade-offs among reliability, entropy, and hardware cost.

To tackle the massive amounts of data generated by IoV apps and any issues with scalability, our method also uses PUFs for key generation and hardware acceleration. PUFs

are developed to improve AV security mechanisms and are very difficult to replicate. They offer unmatched physical protection, low prices, ease of use, outstanding throughput, and low energy consumption, and no one else can match them. On a number of Field-Programmable Gate Array (FPGA) boards, we apply our authentication method that makes use of hardware acceleration. The feasibility of the system is demonstrated by implementing it in VHDL on an FPGA board that has several functionalities. Based on the results of our study, our approach meets all of the necessary requirements for privacy and security in design when compared to other frameworks. Furthermore, to provide an early indication of effectiveness, we summarize key experimental results obtained from both the PUF evaluation and the hardware-based authentication implementation. The proposed heterogeneous PUF demonstrates strong reliability across a wide temperature range, maintaining an average reliability exceeding 98%, while achieving near-ideal randomness and uniqueness values of approximately 49.6% and 49.8%, respectively, which are close to the theoretical optimum of 50%. These results confirm the robustness of the PUF against environmental variations and inter-device correlation. On the hardware side, the complete authentication architecture is implemented on multiple FPGA platforms, where it exhibits low computational overhead and efficient resource utilization, consuming less than 80% of LUT resources on high-capacity devices while maintaining moderate usage of DSPs and on-chip memory. The authentication latency remains sufficiently low to support real-time IoV operations, validating the practicality and scalability of the proposed design. The main contributions of this paper are summarized as follows:

- We propose a privacy-preserving authentication scheme for IoV that enables AVs to authenticate themselves securely while preventing the disclosure of sensitive vehicle identity information to the authentication server.
- We design a bilinear pairing-based searchable encryption scheme that allows AV-generated encrypted authentication requests (trapdoors) to be matched with encrypted vehicle identifiers (indices) stored at the Authentication and Data Collection Server (ADCS), ensuring confidentiality and unlinkability under an honest-but-curious threat model.
- We introduce a heterogeneous, reconfigurable PUF-based key-generation architecture that combines delay-based, ring-oscillator, and SRAM PUF components, along with response preprocessing, routing reconfiguration, and fuzzy extraction, to generate stable, high-entropy cryptographic keys for our proposed authentication scheme.
- We implement the complete authentication scheme using FPGA-based hardware acceleration and validate its feasibility across multiple FPGA platforms, demonstrating low authentication latency and efficient hardware resource utilization.
- We experimentally evaluate the proposed PUF-based design, showing strong reliability, near-ideal randomness, and high uniqueness, confirming its suitability as a hardware root of trust for IoV systems.

The subsequent sections of this paper are structured as follows. Section 2 covers the discussion of related works. Section 3 provides a detailed explanation of our system model. The proposed scheme is described in Section 4. Section 6 presents the performance evaluation. Finally, conclusive insights are provided in Section 7.

2. Related Work

Several schemes have been proposed to enhance the security and privacy of IoV. In [26], the authors proposed a Certificateless Aggregate Signature (CLAS) scheme to make authentication in Vehicular Ad Hoc Networks (VANETs) more efficient. Bundling signatures reduces some of the computational load. However, as the system grows and more vehicles are added, the scheme begins to falter in scalability, making it less effective in larger IoV

setups. In [27], the authors explore the idea of using blockchain for authentication in the IoV. The solution relies on a public key infrastructure (PKI) to secure communication, which is highly secure. However, blockchain brings its own set of issues, like high computational costs and complexity. This can become problematic when applying it to large-scale IoV systems, where you need to keep things efficient and avoid overburdening.

The work in [28] introduces a Certificateless Short Signature Scheme (CLSS) for anonymous authentication of vehicles. It does a good job at protecting user privacy, but the bigger the system gets, the slower and less efficient it becomes. So, while it works well on a small scale, it cannot really handle the size and demands of an extensive IoV system. In [29], the authors take a different approach by using Hardware-Accelerated Authentication (HAA), relying on GPUs to speed up cryptographic processes. This helps boost performance, but the reliance on GPUs brings a hefty price tag and adds complexity to the system, which can make it harder to implement at scale in the real world.

In [30], the authors present an innovative solution for two-factor authentication in IoV systems using PUFs. Their protocol is particularly well-suited to IoV's limited-resource environment, as it pairs PUF responses with user passwords to enable mutual authentication and minimize the risk of offline password-guessing attacks. They also introduce a Key Generation Center (KGC) to manage pseudo-identities and session keys, adding layers of anonymity and traceability to the network. This work aligns with our focus on lightweight, hardware-supported security in IoV. Still, we take it further by integrating bilinear pairing to enable more secure and efficient authentication with hardware acceleration. In [31], the authors introduce a blockchain-based authentication approach that aims to improve security and reduce latency by using decentralized consensus. Unlike traditional IoV systems that rely on a central authority, often resulting in delays, high costs, and data vulnerabilities, this method distributes data across zones managed by local controllers, reducing the need for repeated authentication as vehicles move. However, this scheme has a major scalability limitation: as more vehicles and transactions enter the network, maintaining consensus across zones can slow processing and cause network congestion, especially in busy areas. Moreover, blockchain's high computational demands can strain IoV devices, making it challenging to deliver fast, low-latency authentication in these environments.

The study in [32] examines problems in UAV network security and offers solutions such as intrusion detection. Improving system efficiency, decreasing battery consumption, and identifying unauthorized drones using image-processing algorithms are further areas of focus. The suggested approach is not fit for purpose for real-time authentication in ever-changing IoV settings due to the high processing and latency requirements. Moreover, in contrast to our paper, it does not investigate methods that use hardware acceleration. In [33], new methods for protecting intellectual property (IP) on FPGAs are presented by the authors. The authors explain how to build an intrinsic PUF for FPGAs, examine the statistical features of PUFs based on static random-access memories (SRAMs), discuss the benefits and drawbacks of using a fuzzy extractor, and, lastly, test the design on FPGAs with embedded block RAMs. The permissioned design of Hyperledger Fabric and the consensus overhead it entails cause scalability problems for this method. Its reliance on RSU-based leader selection could also cause delays and bottlenecks in networks that support high-mobility vehicles.

Our approach, using bilinear pairing-based encryption, addresses the shortcomings of these previous schemes. First, unlike blockchain-based methods, our scheme avoids the high computational overhead, making it more practical for large-scale IoV environments. Certificateless cryptography is a good option, but it struggles with large volumes of vehicles, whereas bilinear pairing-based encryption helps manage higher volumes of authentication requests without slowing things down. In addition, using the PUFs to generate the keys

required by our authentication scheme adds another layer of security. On top of that, we use FPGAs for hardware acceleration, which strikes a good balance between cost and performance. This makes our scheme ideal for large, real-time IoV systems that require fast, secure, and scalable authentication.

3. System Model and Design Goals

3.1. Network Model

Our proposed scheme includes three main entities: the Authentication and Data Collection Server (ADCS), Traffic Management Center (TMC), and Autonomous Vehicles (AVs), as illustrated in Figure 1. Each TMC manages a specific traffic zone and oversees AVs within it. AVs communicate with the TMC in their designated zone and transmit essential data, such as location and operational status, via the ADCS server. For secure communication, each AV must first register with the TMC before any data exchange can occur. Then, the TMC will encrypt the AVs' IDs (indices) and send them to the ADCS server. Any AV needs first to send an authentication request (trapdoor) to the ADCS server to authenticate itself before sending its data. Finally, the ADCS server will match the trapdoor to the stored indices without knowing any sensitive AV ID information, and subsequently returns the authentication result to the requesting AV. This step completes the authentication process shown in Figure 1. The ADCS functions as a trusted third-party server known to all network participants. Its primary role is to authenticate AVs before accepting their data, without knowing any sensitive information about them, to preserve their privacy. By centralizing authentication and data handling, the ADCS ensures secure and reliable data flow across the IoV network, safeguarding real-time vehicle-to-infrastructure communication.

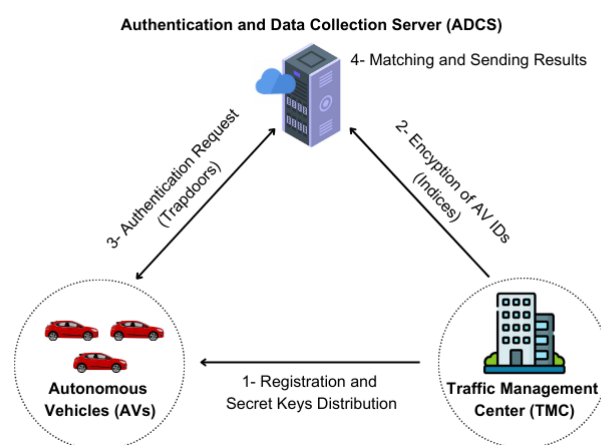


Figure 1. Network model.

3.2. Threat Model

In our scheme, we need to account for both internal and external attackers. Our security model will be honest but curious, where some internal parties, such as the ADCS server and AVs, may follow protocols but still seek additional insight into the system, perhaps curious about details like AV IDs or encryption keys. Even though they are not malicious, their curiosity could inadvertently create security risks. On the other hand, eavesdroppers and other external attackers seeking unauthorized access to the system pose a more urgent threat. Our threat model aligns with the Dolev–Yao (DY) and Canetti–Krawczyk (CK) adversarial models [34,35], which characterize network-level and authentication-related scenarios. In order to protect user privacy within the IoV system, the proposed security goals aim to address and mitigate these risks.

3.3. Design Goals

Considering the aforementioned threat model, the design objectives that our proposed scheme must fulfill are as follows:

- **Scalability and Efficiency:** We need a lightweight encryption and search method that is easy to use. Data retrieval and processing incur less computational and energy expenses as a result of this. The necessary information can be safely accessed by authorized users at the same time. It also improves data encryption and retrieval across different formats and quantities, making it more flexible.
- **Authentication Query Search Over Encrypted AVs' IDs from TMC:** For our method to work, the AV's encrypted authentication requests must be compared with the participating TMC's encrypted identifying data. All AVs are required to encrypt their authentication requests using the same key so that they can match all of the TMC-supplied indices for encrypted data.
- **AVs' ID data and Authentication Query Confidentiality.** The cached AV's encrypted identification data and authentication queries/requests do not include any sensitive or critical information that the ADCS can get.
- **Authentication Query Unlinkability.** The ADCS must be incapable of ascertaining if two authentication requests possess identical or distinct identity data.

4. Proposed Authentication Scheme

Key generation and distribution, AV identification data encryption, authentication query submission, and validation through encrypted data matching make up the four main components of the proposed authentication technique. Table 1 provides the main symbols of our method.

Table 1. Main Notations.

Symbol	Description
PUF	Physical Unclonable Function.
AV	Autonomous Vehicle.
TMC	Transport Management center.
$ADCS$	Authentication and Data Collection Server.
k	Security parameter.
p	Large prime number.
n	Bilinear pairing function.
GR_A, GR_B, GR_C	Multiplicative groups of order p .
$TMSK$	TMC secret key.
$AVSK$	AV secret key.

4.1. Key Generation

In our proposed authentication scheme, the keys are generated through our proposed PUF architecture. The proposed PUF architecture shown in Figure 2 introduces a heterogeneous, reconfigurable design that enhances unpredictability, resistance to modeling attacks, and the reliability of the generated challenge–response pairs (CRPs). The process begins with a digital challenge vector

$$C = [c_1, c_2, \dots, c_n], \quad (1)$$

which passes through a challenge pre-processing unit responsible for scrambling, masking, or permuting the input bits. This preprocessing step transforms the original challenge into a new internal challenge representation $C' = f_{\text{prep}}(C)$, preventing direct correlation attacks and reducing the risk of reverse engineering. By randomizing the mapping between C

and C' , the system introduces an additional security layer before the challenge reaches the PUF fabric.

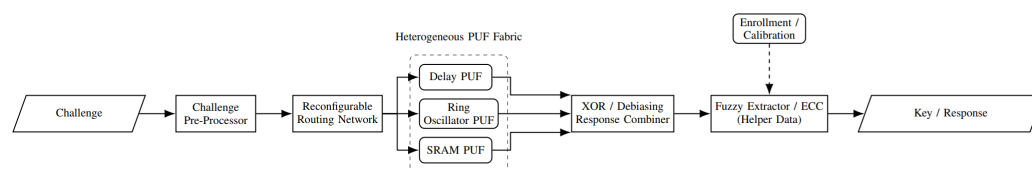


Figure 2. Proposed PUF architecture.

Following preprocessing, the transformed challenge C' is routed into a reconfigurable switching network that dynamically selects the path taken by the signal. This network applies a routing function

$$C'' = f_{\text{route}}(C', S), \quad (2)$$

where S represents the internal reconfiguration state updated periodically or during enrollment. This switching fabric enables multiple possible pathways, creating a large CRP space while mitigating overfitting in machine-learning-based attacks. The reconfigurability also ensures that identical challenges applied at different times may traverse distinct physical paths, further strengthening entropy generation.

In the proposed heterogeneous PUF fabric, each PUF primitive follows a well-defined challenge–response mechanism, tailored to its underlying physical entropy source. In the delay-based PUF, the challenge is a binary vector that configures a set of multiplexers controlling multiple signal propagation paths. Given a challenge $C_d \in \{0, 1\}^n$, two racing signals traverse different paths determined by C_d , and the response $R_d \in \{0, 1\}$ is generated by an arbiter that compares their arrival times. The response can be expressed as $R_d = \text{sign}(\Delta t(C_d))$, where Δt represents the delay difference between the two paths.

For the ring-oscillator (RO) PUF, the challenge C_r selects a pair (or set) of ring oscillators from a pool of available oscillators. The response R_r is obtained by comparing the oscillation frequencies of the selected oscillators over a fixed time window, such that $R_r = 1$ if $f_i > f_j$, and $R_r = 0$ otherwise. Here, the challenge effectively determines which oscillators are activated and compared, enabling a large challenge–response space while maintaining low hardware overhead.

For the SRAM PUF, the challenge C_s corresponds to the address or block selection within the SRAM array that is read during power-up or initialization. Due to intrinsic threshold voltage variations, each SRAM cell exhibits a preferred start-up value, producing a response vector $R_s \in \{0, 1\}^m$. In this case, the challenge does not alter circuit topology but selects which memory locations contribute to the response, enabling flexible response extraction. By combining these independent challenge–response mechanisms through a reconfigurable routing network, the proposed design exploits diverse entropy sources while maintaining a clear and well-defined challenge–response model for each PUF. This heterogeneous approach significantly increases resistance to modeling and cloning attacks compared to relying on a single PUF type.

The routed challenge signals are simultaneously fed into a heterogeneous PUF fabric consisting of three independent entropy sources: a delay-based PUF, a ring-oscillator PUF, and an SRAM-based PUF. Each component produces a raw response bit or vector, denoted by r_{delay} , r_{RO} , r_{SRAM} . These responses arise from different types of manufacturing variations, path delays, oscillator frequency mismatches, and power-up memory state biases, which collectively yield complementary entropy characteristics. The three raw responses are combined through an XOR-based debiasing function,

$$r_{\text{comb}} = r_{\text{delay}} \oplus r_{\text{RO}} \oplus r_{\text{SRAM}}, \quad (3)$$

which suppresses structural bias, increases unpredictability, and makes modeling attacks substantially more difficult.

Finally, the combined response r_{comb} is processed through a fuzzy extractor that performs error correction, helper-data generation, and key reconstruction. Since environmental variations may introduce noise in the physical measurements, the fuzzy extractor applies an error-correcting code (ECC) to reconstruct a stable key. Let w be the noisy combined response and h be the stored helper data; then, the recovered secret key is obtained using

$$K = \text{FE}(w, h), \quad (4)$$

where $\text{FE}(\cdot)$ denotes the fuzzy extractor reconstruction function. This produces a deterministic and reliable key despite inherent hardware noise. The enrollment block provides initial calibration, generates helper data, and stores system parameters for long-term operation. Overall, this novel PUF design combines preprocessing, reconfigurable routing, heterogeneous entropy sources, and strong post-processing to deliver a secure, robust, and machine-learning-resistant hardware root of trust.

The motivation for adopting a hybrid PUF architecture composed of three distinct PUF types, namely, delay-based, ring-oscillator, and SRAM PUFs, is to exploit complementary and independent sources of physical entropy while mitigating the inherent weaknesses of any single or dual-PUF configuration. Each PUF type is subject to different classes of attacks and reliability challenges: delay-based PUFs are susceptible to machine-learning modeling attacks, ring-oscillator PUFs may suffer from frequency aging and environmental sensitivity, and SRAM PUFs typically offer a limited challenge space. By integrating all three PUFs, the proposed design introduces orthogonal entropy sources arising from path-delay variations, oscillation-frequency mismatches, and memory-cell power-up states, respectively. From a security perspective, combining three independent PUFs significantly enlarges the effective challenge–response space and increases the complexity of constructing an accurate attack model. An adversary must simultaneously characterize multiple, statistically independent physical phenomena to predict the composite response, a task that is substantially more difficult than modeling one or two correlated PUF sources. Furthermore, even if one PUF instance becomes partially predictable or degraded over time, the remaining PUFs continue to contribute fresh entropy, preserving the overall robustness of the authentication process.

4.2. Key Distribution

The TMC initiates the system setup algorithm by taking the security parameter k as input and produces $\{\mathbb{G}_{R_A}, \mathbb{G}_{R_B}, \mathbb{G}_{R_C}, p, n\}$, where p is a large prime number, $\mathbb{G}_{R_A}$, $\mathbb{G}_{R_B}$, and $\mathbb{G}_{R_C}$ are multiplicative groups of order p , and $n : \mathbb{G}_{R_A} \times \mathbb{G}_{R_B} \rightarrow \mathbb{G}_{R_C}$. It also selects generators $u_1 \in \mathbb{G}_{R_A}$ and $u_2 \in \mathbb{G}_{R_B}$. Then, it uses K , the output of proposed PUF design. Also, it samples $R_1 \leftarrow \mathbb{Z}_p^{k \times k}$, $R_2 \leftarrow \mathbb{Z}_p^{k \times k}$ from the field $\mathbb{Z}_p$. Finally, the setup algorithm outputs the public parameters $\text{pub} = (\mathbb{G}_{R_A}, \mathbb{G}_{R_B}, \mathbb{G}_{R_C}, u_1, u_2, p, n)$, and the TMC secret key $(TMSK) = (KR_1, KR_2)$.

The TMC then computes the secret key of each AV (AV) in the system as follows. It samples K' and K'' from $\mathbb{Z}_p^{k \times k}$ such that $K' + K'' = K^{-1}$ and outputs the secret key as $AVSK = (R_1^{-1}K', R_2^{-1}K'')$. Note that for each AV to have a different secret key, K' and K'' are unique for each AV. Each AV then registers its ID data with the TMC.

4.3. Uploading Encrypted AVs' IDs

The TMC creates a collection of encrypted indices as the encryption of AVs' ID information using its corresponding key $TMSK$. For each AV (with ID AV_i), the TMC creates J_i for its encrypted ID information of size k . The TMC samples $\gamma \leftarrow \mathbb{Z}_p$ and generates the

index as: $J_i = (u_1^\gamma, u_1^{\gamma \cdot AV_i \cdot KR_1}, u_1^{\gamma \cdot AV_i \cdot KR_2})$. Then, the TMC sends J_i to the ADCS for future use in the authentication process.

4.4. AV Authentication Request

For any AV that wants to send its data to the system, it first encrypts its ID (Y_j) by sampling $\delta \leftarrow \mathbb{Z}_p$ and generates its trapdoor as: $U_j = (u_2^\delta, u_2^{\delta \cdot R_1^{-1} K' \cdot Y_j^T}, u_2^{\delta \cdot R_2^{-1} K'' \cdot Y_j^T})$. Then, U_j is sent to the ADCS for authentication and matching. When many authentication requests are sent by the same AV, the ADCS is unable to connect them. To achieve unlinkability, the sampling process (δ) must be random. It is difficult to correlate queries to the same AV because each authentication request appears different.

4.5. Authentication Results

Finally, the ADCS conducts a secure dot product operation between the trapdoor U_j and each stored index J_i . The following is computed by the server:

1. $F_1 = n(u_1^\gamma, u_2^\delta) = n(u_1, u_2)^{\gamma\delta}$
2. $F_2 = n(u_1^{\gamma \cdot AV_i \cdot KR_1}, u_2^{\delta \cdot R_1^{-1} K' \cdot Y_j^T})$
 $= n(u_1, u_2)^{\gamma\delta \cdot AV_i \cdot KR_1 R_1^{-1} K' \cdot Y_j^T}$
 $= n(u_1, u_2)^{\gamma\delta \cdot AV_i \cdot KK' \cdot Y_j^T}$
3. $F_3 = n(u_1^{\gamma \cdot AV_i \cdot KR_2}, u_2^{\delta \cdot R_2^{-1} K'' \cdot Y_j^T})$
 $= n(u_1, u_2)^{\gamma\delta \cdot AV_i \cdot KR_2 R_2^{-1} K'' \cdot Y_j^T}$
 $= n(u_1, u_2)^{\gamma\delta \cdot AV_i \cdot KK'' \cdot Y_j^T}$
4. $F_4 = F_2 * F_3$
 $= n(u_1, u_2)^{\gamma\delta \cdot AV_i \cdot KK' \cdot Y_j^T + \gamma\delta \cdot AV_i \cdot KK'' \cdot Y_j^T}$
 $= n(u_1, u_2)^{\gamma\delta \cdot \langle AV_i \cdot (KK' + KK'') \cdot Y_j^T \rangle}$
 $= n(u_1, u_2)^{\gamma\delta \cdot \langle AV_i \cdot K(K' + K'') \cdot Y_j^T \rangle}$
 $= n(u_1, u_2)^{\gamma\delta \cdot \langle AV_i \cdot KK^{-1} \cdot Y_j^T \rangle}$
 $= n(u_1, u_2)^{\gamma\delta \cdot \langle AV_i \cdot Y_j^T \rangle}$
 $= n(u_1, u_2)^{\gamma\delta \cdot \langle AV_i \cdot Y_j \rangle} = F_1^{\langle AV_i \cdot Y_j \rangle}$
5. Knowing F_1 and F_4 , we calculate $\text{Discrete log}(F_4, F_1) \longrightarrow \langle AV_i \cdot Y_j \rangle$ to authenticate the AV (Y_j belonging to AV_i).

5. Security and Privacy Analysis

In accordance with the design objectives in Section 3.3, we demonstrate that our proposed scheme meets all designated capabilities and requirements by effectively addressing each design goal.

- **Scalability and Efficiency.**

The suggested system efficiently searches encrypted IDs from the TMC and quickly addresses requests from the AVs. This is achieved by performing a dot product on the relevant encrypted IDs, using hardware acceleration. Furthermore, the computational requirements of our approach are relatively moderate. This efficiency follows directly from the construction of encrypted indices J_i and authentication trapdoors U_j , which enable the ADCS to verify requests through secure dot product operations without decryption, as shown in Section 4.5.

- **Authentication Query Search Over Encrypted AVs' IDs from the TMC.**

Our proposed authentication scheme is based on searching over encrypted AV IDs, rather than traditional key-based authentication schemes, which limit exposure of

sensitive identity information even to internal entities. The proposed approach employs encrypted authentication queries transmitted from an AV to the ADCS to search encrypted ID data from a participating TMC entity. Each AV utilizes a unique key to encrypt its authentication request, hence facilitating the matching of all indices supplied by the TMC for the extraction of encrypted data. Specifically, the TMC uploads encrypted indices J_i generated using its secret key $TMSK$, while each AV submits a trapdoor U_j constructed by using its secret key $AVSK$, enabling authentication through encrypted-domain matching rather than key-based identity verification. In addition, all sensitive communications are protected using encryption, thereby defending against eavesdropping attacks by external adversaries. So, as long as the TMC secret key ($TMSK$) and AV secret key ($AVSK$), kept secret (based on our proposed PUF design), no attackers can see or change any AV's ID information.

- **AVs'ID data and Authentication Query Confidentiality.**

When it comes to stored ID data or issued authentication requests, the ADCS cannot access any potentially sensitive or critical information. The AV and TMC's encryption makes this possible. By encrypting them, IDs and authentication requests are protected from being sent to the ADCS in plaintext. By performing searches solely within the encrypted data, our scheme increases data privacy while the server refrains from decrypting it. Besides the security of the keys (generated by our proposed PUF design) used in the encryption process for the AVs' IDs submitted by the TMC and the authentication request submitted by an AV, confidentiality is ensured also by the use of multiplicative group operations and randomization parameters γ and δ , which prevent the ADCS from recovering AVs' identities or authentication request contents.

- **Authentication Query Unlinkability.**

It is not possible for the ADCS to determine whether two authentication requests contain the same identification data. By leveraging the randomness of the sampling (δ), our approach ensures that authentication queries cannot be linked by generating distinct ciphertexts for the same AV ID. As each trapdoor U_j is generated using fresh randomness, repeated authentication attempts by the same AV produce unlinkable ciphertexts.

It is important to note that the security of the proposed authentication scheme does not rely on the secrecy of the protocol itself, but rather on the secrecy of the cryptographic keys. In accordance with standard cryptographic principles, the details of the authentication scheme and its underlying algorithms may be fully known to internal or external attackers without compromising security. In the proposed framework, even if an attacker is aware of the authentication process, bilinear pairing operations, and PUF-based key generation mechanism, successful attacks remain infeasible without access to the correct secret keys. These keys are generated using the proposed PUF architecture and are never exposed in plaintext to the authentication server or to other network entities. As a result, attackers cannot encrypt valid authentication requests, decrypt stored identifiers, or link authentication queries to specific vehicles. Therefore, the overall security of the scheme fundamentally depends on the secret keys rather than on the protocol's obscurity.

6. Implementation and Experimental Results

6.1. Hardware Architecture

When an AV and an ADCS exchange data, the proposed method establishes authentication. Figure 3 shows the block diagram of the suggested methodology. Every AV has its own unique identifier, which is generated internally by an ID generator. For m vehicles, this identifier might range from 64 bits to 128 bits. The ID generator's output is saved in the corresponding AV register; for instance, R-v1 is associated with AV1 and R-v2 is designated

with AV2. Each AV is assigned a unique key by the TMC, which is then stored in a register with m locations that correspond to the m vehicle numbers; for instance, the keys for AV1 and AV2 are kept in R-k1 and R-k2, respectively. Separate multiplexers are used to link the ID register and the key register. By utilizing the identical selection signal produced by a control unit, multiplexers transmit the required ID together with its matching key.

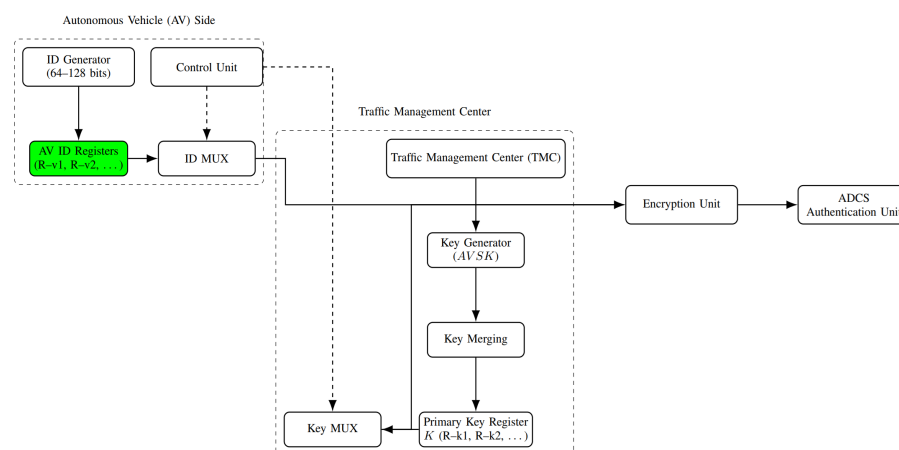


Figure 3. Block diagram of the proposed method.

The registration and encryption processes of each AV are handled by the control unit. A unique identifier is created for each AV by the ID generator whenever a new AV is added to the network. The new vehicle ID is transmitted to the TMC for registration by means of a multiplexer selection signal generated by the control unit. Assume the vehicles are unchanged and that an AV must encrypt its identification data. In order to communicate with the encryption unit, the control unit generates selection signals for the ID and key multiplexers. These signals specify which AV's ID and key are necessary.

As shown in Figure 3, the TMC is formed of many blocks that can generate new keys and encrypt an AV's ID with a key ($AVSK$). The primary key K register stores all keys and is utilized in the hardware implementation to access the key needed for the following operations. The TMC receives an identifier (ID) from the AV during registration and stores it in a buffer until it can be sent to an ID registration unit controlled by the control unit. The control unit specifies where the new ID must be registered. The key-merging block takes all keys and merges them into a single primary key K . After receiving this ID, a key generator generates a new key $AVSK$. All of these processes are managed and coordinated by the control unit. In order to transmit the ID and key K to the encryption unit, the control unit uses the ID register and the key register during the encryption phase. The ADCS receives the encrypted data. Encrypted identification data received from an AV must be matched with encrypted information from the TMC as part of the ADCS task. The authentication outcome permits data acceptance if the encrypted vehicle ID corresponds to entries in the ADCS.

6.2. Experimental Results

6.2.1. Communication Overhead

The size of the key and each index or trapdoor contribute to the communication overhead. This process makes use of a 265-bit asymmetric pairing curve (BN256) with a 32-byte group element size. An encrypted vector, that can act as either an index or a trapdoor, has a length of $(2n + 1)$ group items, with n being the size of the ID. If the key size is 64 bits, the index or trapdoor will be 129×32 bytes (4128), and if it is 128 bits, it will be 257×32 bytes (8224). Two matrices, each holding $n \times n$ items, make up the key size for an ID size of n bits. The total key size for a 64 ID is 131,072 bytes, with 16 bytes allotted to each

data item, determined by multiplying $2 \times 64 \times 64 \times 16$ bytes. The overall key size, measured in bytes, is 524,288 for a key size of 128 bits, determined as $2 \times 128 \times 128 \times 16$ bytes. Given the existing methods, these outcomes are acceptable.

6.2.2. Computation Overhead

The encryption-time performance of the proposed authentication scheme is shown in Figure 4. As the AV ID size (key size as the output of the PUF) increases from 100 to 800 bits, the encryption time grows gradually and nearly linearly, rising from 0.45 ms to 2.32 ms. This behavior indicates that the encryption module's computational complexity scales efficiently with the input size. The moderate slope of the curve demonstrates that the proposed design can accommodate larger identifier sizes without incurring a significant performance penalty, which is essential for supporting diverse security requirements in IoV environments. Moreover, the sub-millisecond encryption time for IDs up to 300 bits highlights the scheme's suitability for real-time authentication scenarios, where low latency is a critical requirement for autonomous vehicle communications. This behavior confirms that the encryption module operates with linear time complexity, i.e., $\mathcal{O}(n)$, where n denotes the ID length. Figure 5 shows the search-time performance versus ID size for the proposed authentication scheme. The results show that the search time remains in the microsecond range even as the ID size increases, ranging from 0.10 μs for 100 bits to 1.30 μs for 800 bits. This low-latency behavior confirms the efficiency of the ID matching and lookup mechanism implemented within the authentication framework. The modest increase in search time suggests that the proposed design can support large-scale AV deployments with minimal delay, ensuring fast authentication decisions and maintaining system scalability under dense vehicular network conditions.

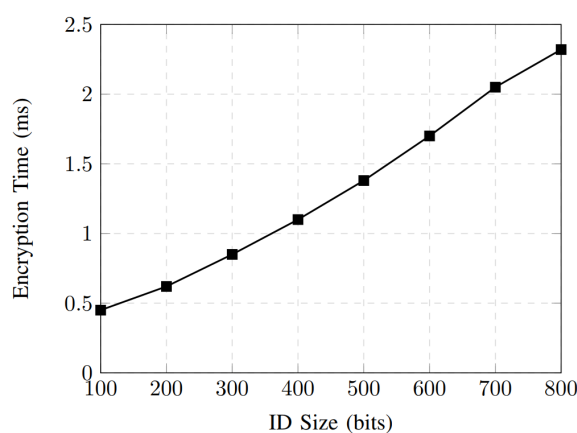


Figure 4. Encryption time performance.

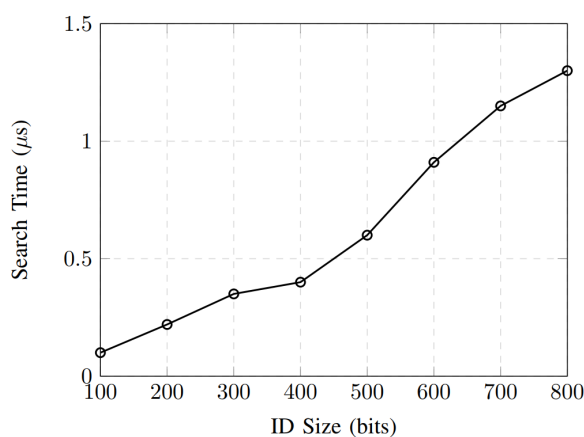


Figure 5. Searching time performance.

6.2.3. Hardware Resource Utilization

The hardware-accelerated authentication technique is executed in VHDL across three distinct FPGAs. The hardware's cost and performance are analyzed. The initial implementation is executed on the Nexys A7-100T FPGA, priced at \$349. The second implementation is executed on the Zynq Ultrascale+ ZCU104 FPGA, priced at \$1678. The Kintex Ultrascale+ 116 is the third FPGA, with a valuation of \$3882. We used the same methodology across varying FPGA prices and resources and conducted a performance and cost comparison. Resource usage is assessed for each FPGA implementation. We quantified the resources utilized by the authentication method, and the ratio of utilized resources to available resources is shown in Figure 6. The Kintex 116 FPGA accommodates substantial ID sizes (an elevated security level) and offers greater resources than alternative FPGAs for the authentication method; nonetheless, it incurs a higher cost. The Nexys 100T FPGA is utilized for modest ID sizes (low-security level) due to its limited resources and low cost. The mid-range is implemented on the Zynq104 FPGA due to its moderate performance and affordability. This study showcases many uses of the hardware-accelerated authentication mechanism to facilitate diverse AV resources in the IoV era.

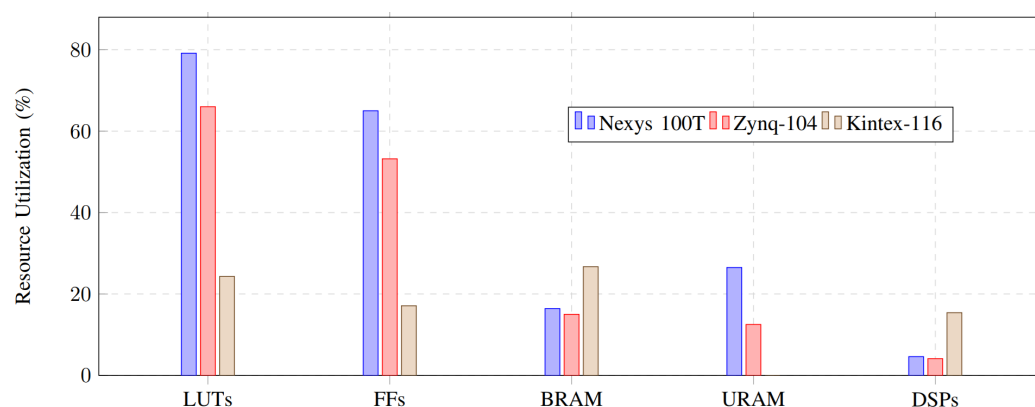


Figure 6. Overall hardware resource utilization of the proposed authentication scheme across different FPGA platforms.

Although the proposed heterogeneous PUF fabric integrates three independent entropy sources, namely a delay-based PUF, a ring-oscillator PUF, and an SRAM-based PUF, the overall hardware cost remains practical and well within the capabilities of modern FPGA platforms. Each PUF primitive is lightweight by design: the delay-based PUF relies primarily on configurable routing and simple arbiters; the ring-oscillator PUF uses a limited number of inverters and counters; and the SRAM PUF leverages existing on-chip memory blocks without requiring additional custom circuitry. As demonstrated by the FPGA synthesis results, the complete authentication architecture, including the heterogeneous PUF fabric, consumes a modest portion of logic and memory resources, with DSP utilization remaining below 16% and memory usage below 27% across evaluated platforms. Furthermore, the PUF components are not operated concurrently; instead, the reconfigurable routing network selectively activates individual PUF instances, which further reduces dynamic power consumption and hardware overhead. These characteristics confirm that the proposed heterogeneous PUF is feasible for practical deployment and offers a favorable trade-off between hardware cost and security enhancement in real-world autonomous vehicular systems.

6.2.4. PUF Performance Analysis

The results summarized in Table 2 demonstrate that the proposed heterogeneous PUF design achieves strong statistical performance across the most critical security metrics.

The uniqueness metric, measured at 49.2%, is very close to the theoretical ideal of 50%, indicating that PUF instances from different chips produce highly distinguishable responses. Likewise, the reliability measures show that the design delivers stable response bits across environmental variations, including temperature, voltage, and aging, achieving 97.8% stability. These metrics confirm that the joint operation of the reconfigurable routing network and the mixed PUF fabric effectively reduces noise and path imbalance.

Table 2. Evaluation Results of the Novel Heterogeneous PUF.

Metric	Expected Ideal	Measured Value	Interpretation
Uniqueness (%)	50	49.2	Excellent inter-chip variation
Reliability (%)	100	97.8	Stable responses under noise
Bit-Aliasing (%)	50	50.6	No structural bias across bits
Uniformity (%)	50	49.8	Balanced 0/1 distribution
Entropy (bits)	n	$0.994n$	Near-ideal randomness per bit
Steadiness (%)	100	98.5	Strong resilience after ECC

The remaining statistical indicators, bit-aliasing, uniformity, entropy, and steadiness, also reinforce the robustness of the design. The uniformity and bit-aliasing results, at 49.8% and 50.6%, respectively, suggest that the PUF output is unbiased and does not favor specific bit positions across chips. The entropy level of $0.994n$ shows that the combined PUF elements, when processed through the XOR/combiner and fuzzy extractor, generate nearly ideal randomness. Furthermore, the steadiness score of 98.5% after fuzzy extraction indicates that the error-correction subsystem successfully mitigates instability arising from individual PUF components. Together, these results validate the strength of the proposed architecture in providing secure, stable, and high-quality challenge–response behavior.

Figure 7 illustrates the reliability comparison between the proposed PUF and a traditional PUF across a wide temperature range. Reliability is defined as the probability that the same response is reproduced under varying environmental conditions for a fixed challenge. As observed, the proposed PUF maintains consistently higher reliability as temperature deviates from the nominal operating point. This improvement is mainly attributed to the heterogeneous PUF fabric and the response stabilization stage, which mitigates temperature-induced delay variations and metastability effects. Furthermore, incorporating a fuzzy extractor with error correction ensures that minor bit flips caused by thermal noise are corrected, leading to near-ideal reliability even at elevated temperatures. In contrast, the traditional PUF exhibits a noticeable degradation in reliability as temperature increases, highlighting its sensitivity to environmental variations.

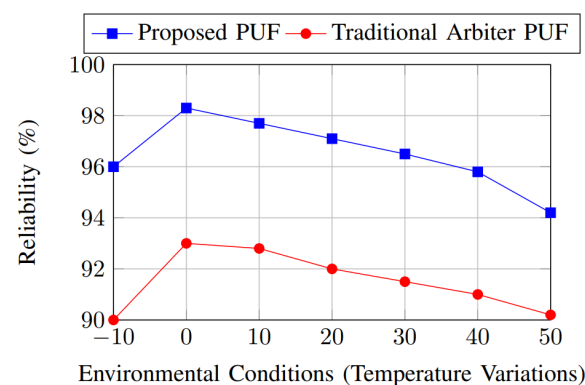


Figure 7. Reliability comparison.

The randomness comparison shown in Figure 8 evaluates the statistical balance of the PUF responses across different challenge sets. Randomness is measured as the ratio of logic '1's to the total response length, with an ideal value close to 50%. The proposed PUF demonstrates randomness that remains tightly centered around the ideal value for all evaluated challenge sets, indicating strong resistance to bias. This behavior is achieved through the combined effects of reconfigurable routing, heterogeneous PUF cores, and XOR-based response combining, which collectively decorrelate structural dependencies within individual PUF primitives. In comparison, the traditional PUF exhibits larger fluctuations in randomness across challenge sets, suggesting greater susceptibility to systematic bias and correlated responses.

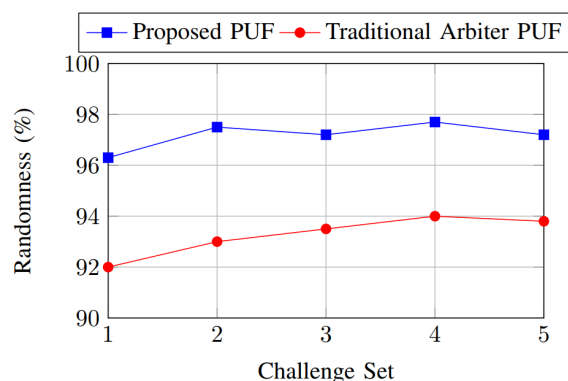


Figure 8. Randomness comparison.

Figure 9 presents the uniqueness results for the proposed and traditional PUFs as the number of evaluated PUF instances increases. Uniqueness is quantified as the average inter-device Hamming distance between responses to identical challenges, with an ideal value of 50%. The proposed PUF achieves unique values that closely approach the ideal target across the entire PUF set, demonstrating substantial inter-chip variability. This improvement is primarily due to the heterogeneous nature of the PUF fabric, which amplifies manufacturing variations across multiple physical entropy sources. Additionally, the reconfigurable routing network further enhances diversity by altering signal paths on a per-instance basis. In contrast, the traditional PUF exhibits lower and less stable uniqueness values, indicating reduced resistance to device cloning and modeling attacks.

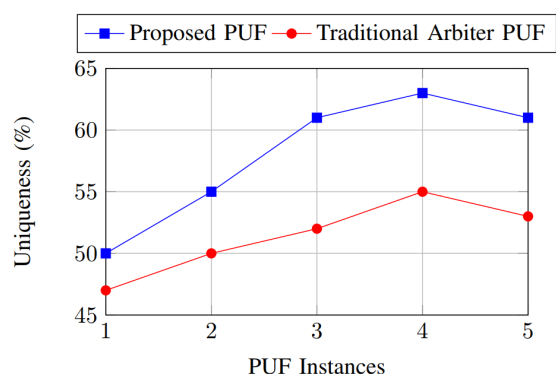


Figure 9. Uniqueness comparison.

The randomness of the proposed PUF is evaluated using the average Hamming weight, which measures the balance between logic '0' and logic '1' in the generated responses. For

an n -bit PUF response $\mathbf{R} = \{r_1, r_2, \dots, r_n\}$, the Hamming weight is defined as $\text{HW}(\mathbf{R}) = \sum_{i=1}^n r_i$, and the normalized average Hamming weight [36] is expressed as

$$\text{HW}_{\text{avg}} = \frac{1}{n} \sum_{i=1}^n r_i \times 100\%. \quad (5)$$

Experimental evaluation of the proposed design over multiple challenge sets yields an average Hamming weight of 49.7%, which is close to the ideal value.

Table 3 presents a quantitative comparison between the proposed PUF-based authentication method and several recent state-of-the-art designs in terms of uniqueness, reliability, and uniformity. The proposed method achieves a uniqueness of 49.2%, which is very close to the ideal value of 50% and comparable to the best-performing prior work, indicating strong inter-device distinguishability. In terms of reliability, the proposed design outperforms existing schemes, achieving 97.8% and demonstrating robust, stable response generation under environmental and operating variations. Furthermore, the uniformity of the proposed method reaches 49.8%, closely approximating the ideal distribution and improving upon [37], while maintaining comparable performance to [38]. Overall, the results confirm that the proposed approach provides a well-balanced improvement across all key PUF metrics, making it more suitable for secure, reliable authentication in resource-constrained, safety-critical IoV environments.

Table 3. Comparison with existing works.

Ref.	Uniqueness	Reliability	Uniformity
[37]	45.25	95.93	48.30
[38]	49	85.95	50
[39]	41.53	95.50	N/A
The proposed method	49.2	97.8	49.8

7. Conclusions

With the rise of IoV services, ensuring security and privacy has become essential. This paper introduces a novel privacy-preserving authentication mechanism for AVs within the IoV domain, utilizing physical unclonable functions (PUFs). This strategy uses a bilinear-pairing-based encryption method to facilitate search within encrypted data. The principal objective of this scheme is to verify the authenticity of AVs inside the IoV framework. A revolutionary PUF architecture produces random keys for our authentication method, hence enhancing security. This dual-layer security approach protects against many cyber risks, such as identity theft, man-in-the-middle attacks, and unauthorized access to confidential user information. The PUF design will ensure the genuine randomization of the secret keys for AV users. To manage the substantial volume of data, we employ hardware acceleration via FPGAs. Our security and privacy evaluation demonstrates that the scheme effectively authenticates data sources without revealing any sensitive information. Moreover, by using hardware acceleration, we achieved substantial reductions in computational and communication overhead, making this solution both efficient and practical for real-time IoV needs.

Author Contributions: Conceptualization, R.F., U.M., A.S., M.H. and K.K.; Methodology, R.F., U.M., A.S., M.H., N.R. and K.K.; Software, R.F., U.M., A.S., M.H. and K.K.; Validation, R.F., A.S., N.R. and K.K.; Formal analysis, R.F., U.M., A.S., M.H. and K.K.; Investigation, R.F., U.M., A.S., M.H., N.R. and K.K.; Resources, A.S. and K.K.; Data curation, A.S.; Writing – original draft, R.F., U.M., A.S. and K.K.; Writing – review & editing, A.S.; Visualization, R.F., U.M., A.S. and K.K.; Supervision, A.S.; Project administration, A.S. 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.

Acknowledgments: The Security and Privacy of Emerging Network (SPEN) research lab at the University of Southern Mississippi (USM), USA, made this work possible. The statements made herein are solely the responsibility of the authors.

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

References

1. Rani, P.; Sharma, R. Intelligent transportation system for internet of vehicles based vehicular networks for smart cities. *Comput. Electr. Eng.* **2023**, *105*, 108543. <https://doi.org/10.1016/j.compeleceng.2022.108543>.
2. Lan, Y.H.; Zhao, J.Y. Improving Track Performance by Combining Padé-Approximation-Based Preview Repetitive Control and Equivalent-Input-Disturbance. *J. Electr. Eng. Technol.* **2024**, *19*, 3781–3794. <https://doi.org/10.1007/s42835-024-01830-x>.
3. Ding, C.; Zhu, L.; Shen, L.; Li, Z.; Li, Y.; Liang, Q. The Intelligent Traffic Flow Control System Based on 6G and Optimized Genetic Algorithm. *IEEE Trans. Intell. Transp. Syst.* **2024**, *26*, 17403–17416. <https://doi.org/10.1109/TITS.2024.3467269>.
4. Hu, J.; Jiang, H.; Chen, S.; Zhang, Q.; Xiao, Z.; Liu, D.; Liu, J.; Li, B. WiShield: Privacy Against Wi-Fi Human Tracking. *IEEE J. Sel. Areas Commun.* **2024**, *42*, 2970–2984. <https://doi.org/10.1109/JSAC.2024.3414597>.
5. Xu, J.; Li, M.; He, Z.; Anwlnkom, T. Security and privacy protection communication protocol for Internet of vehicles in smart cities. *Comput. Electr. Eng.* **2023**, *109*, 108778. <https://doi.org/10.1016/j.compeleceng.2023.108778>.
6. Liu, Y.; Zhao, Y. A Blockchain-Enabled Framework for Vehicular Data Sensing: Enhancing Information Freshness. *IEEE Trans. Veh. Technol.* **2024**, *73*, 17416–17429. <https://doi.org/10.1109/TVT.2024.3417689>.
7. Zhang, M.; Wei, E.; Berry, R.; Huang, J. Age-Dependent Differential Privacy. *IEEE Trans. Inf. Theory* **2024**, *70*, 1300–1319. <https://doi.org/10.1109/TIT.2023.3340147>.
8. Gong, Y.; Yao, H.; Liu, X.; Bennis, M.; Nallanathan, A.; Han, Z. Computation and Privacy Protection for Satellite-Ground Digital Twin Networks. *IEEE Trans. Commun.* **2024**, *72*, 5532–5546. <https://doi.org/10.1109/TCOMM.2024.3392795>.
9. Abbass, M.; Sherif, A.; Riley, J.; Khalil, K. AI-Powered Secure and Privacy-Aware Maintenance Prediction Scheme for Autonomous Vehicles Using Hardware Acceleration. *IEEE Internet Things J.* **2025**, *13*, 5305–5319.
10. Madububa Mbachu, U.; Fatima, R.; Sherif, A.; Dockery, E.; Mahmoud, M.; Alsabaan, M.; Khalil, K. Hardware Acceleration-Based Privacy-Aware Authentication Scheme for Internet of Vehicles Using Physical Unclonable Function. *Sensors* **2025**, *25*, 1629.
11. Madububambachu, U.; Fatima, R.; White, K.; Riley, J.; Sherif, A.; Khalil, K. Hardware-acceleration based privacy-aware authentication scheme for internet of vehicles. In *Proceedings of the 2024 IEEE 3rd International Conference on Computing and Machine Intelligence (ICMI)*; IEEE: Piscataway, NJ, USA, 2024; pp. 1–5.
12. Drobot, A.; Zhang, T.; Buonarosa, M.L.; Kargl, F.; Schwinke, S.; Sikdar, B. The Internet of Vehicles (IoV)—Security, Privacy, Trust, and Reputation Management for Connected Vehicles. *IEEE Internet Things Mag.* **2023**, *6*, 6–16. <https://doi.org/10.1109/MIOT.2023.10145018>.
13. Zhou, Q.; Zeng, Z.; Wang, K.; Chen, M.; Zheng, Y. Privacy Protection Scheme for the Internet of Vehicles Based on Collaborative Services. *IEEE Internet Things J.* **2023**, *10*, 13342–13353. <https://doi.org/10.1109/JIOT.2023.3262827>.
14. Khalil, K.; Kumar, A.; Bayoumi, M. Hardware Acceleration of CoAP Protocol for High-Speed and Low-Power Internet of Things Communication. *IEEE Internet Things J.* **2025**, *12*, 8206–8218. <https://doi.org/10.1109/JIOT.2024.3502549>.
15. Madububambachu, U.; Fatima, R.; Sherif, A.; Khalil, K. Security and Privacy Solutions in Intelligent Transportation Systems: A Survey. *Internet Things* **2025**, *34*, 101812.
16. Seliem, M.; Elgazzar, K.; Khalil, K. Towards privacy preserving iot environments: A survey. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 1032761.
17. Akter, S.; Khalil, K.; Bayoumi, M. A survey on hardware security: Current trends and challenges. *IEEE Access* **2023**, *11*, 77543–77565.
18. Khalil, K.; Idriss, H.; Idriss, T.; Bayoumi, M. *Lightweight Hardware Security and Physically Unclonable Functions*; Springer: Cham, Switzerland, 2025.
19. Younes, L.; Abulibdeh, E.; Mohammad, B.; Saleh, H.; Al-Qutayri, M. DCDC PUF an enhanced implementation of ring oscillator based PUF. *Sci. Rep.* **2025**, *15*, 31017.
20. Khalil, K.; Idriss, H.; Idriss, T.; Bayoumi, M. Advanced PUF Designs. In *Lightweight Hardware Security and Physically Unclonable Functions: Improving Security of Constrained IoT Devices*; Springer: Cham, Switzerland, 2025; pp. 97–113.

21. Alahmadi, S.; Khalil, K.; Bayoumi, M. Enhancing arbiter PUF against modeling attacks using constant weight encoding. In *Proceedings of the 2024 IEEE 67th International Midwest Symposium on Circuits and Systems (MWSCAS)*; IEEE: Piscataway, NJ, USA, 2024; pp. 173–177.
22. Jia, C.; Tan, W.; Shen, A.; Li, Z.; Chen, Y.; Zhao, R.; Niu, Q.; Li, C. A puf-enhanced fog-enabled hierarchical authentication protocol for internet of vehicles. *IEEE Internet Things J.* **2025**, *12*, 37629–37644.
23. Alahmadi, S.; Khalil, K.; Idriss, H.; Bayoumi, M. Fortifying strong pufs: A modeling attack-resilient approach using weak puf for iot device security. In *Proceedings of the 2024 IEEE International Symposium on Circuits and Systems (ISCAS)*; IEEE: Piscataway, NJ, USA, 2024; pp. 1–5.
24. Khalil, K.; Idriss, H.; Idriss, T.; Bayoumi, M. Hardware Security Challenges. In *Lightweight Hardware Security and Physically Unclonable Functions: Improving Security of Constrained IoT Devices*; Springer: Cham, Switzerland, 2025; pp. 35–40.
25. Dey, B.; Khalil, K.; Kumar, A.; Bayoumi, M. A novel design gate based low-cost configurable ro puf using reversible logic. In *Proceedings of the 2019 IEEE 62nd International Midwest Symposium on Circuits and Systems (MWSCAS)*; IEEE: Piscataway, NJ, USA, 2019; pp. 211–214.
26. Zhong, H.; Han, S.; Cui, J.; Zhang, J.; Xu, Y. Privacy-preserving authentication scheme with full aggregation in VANET. *Inf. Sci.* **2019**, *476*, 211–221. <https://doi.org/10.1016/j.ins.2018.10.021>.
27. Wang, X.; Zeng, P.; Patterson, N.; Jiang, F.; Doss, R. An Improved Authentication Scheme for Internet of Vehicles Based on Blockchain Technology. *IEEE Access* **2019**, *7*, 45061–45072. <https://doi.org/10.1109/ACCESS.2019.2909004>.
28. Liu, J.; Li, Q.; Sun, R.; Du, X.; Guizani, M. An Efficient Anonymous Authentication Scheme for Internet of Vehicles. In *Proceedings of the 2018 IEEE International Conference on Communications (ICC)*; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6. <https://doi.org/10.1109/ICC.2018.8422447>.
29. Singla, A.; Mudgerikar, A.; Papapanagiotou, I.; Yavuz, A.A. HAA: Hardware-Accelerated Authentication for internet of things in mission critical vehicular networks. In *Proceedings of the MILCOM 2015–2015 IEEE Military Communications Conference*; IEEE: Piscataway, NJ, USA, 2015; pp. 1298–1304. <https://doi.org/10.1109/MILCOM.2015.7357624>.
30. Tian, Z.; He, Y.; Liu, Y.; Liu, S.; Quan, J. Two-factor authentication protocol based on PUF function in Internet of Vehicles. In *Proceedings of the 2023 6th International Conference on Artificial Intelligence and Pattern Recognition*; Association for Computing Machinery: New York, NY, USA, 2024; pp. 1083–1090. <https://doi.org/10.1145/3641584.3641745>.
31. Yu, H.; Tu, S.; Zhang, Y. Decentralized Consensus Blockchain-Based Authentication Algorithm Using in Secure Internet of Vehicles. In *Proceedings of the 2022 12th International Conference on Communication and Network Security*; Association for Computing Machinery: New York, NY, USA, 2023; pp. 199–204. <https://doi.org/10.1145/3586102.3586132>.
32. Abualsauod, E.H. A hybrid blockchain method in internet of things for privacy and security in unmanned aerial vehicles network. *Comput. Electr. Eng.* **2022**, *99*, 107847. <https://doi.org/10.1016/j.compeleceng.2022.107847>.
33. Qureshi, K.N.; Shahzad, L.; Abdelmaboud, A.; Elfadil Eisa, T.A.; Alamri, B.; Javed, I.T.; Al-Dhaqm, A.; Crespi, N. A Blockchain-Based Efficient, Secure and Anonymous Conditional Privacy-Preserving and Authentication Scheme for the Internet of Vehicles. *Appl. Sci.* **2022**, *12*, 476. <https://doi.org/10.3390/app12010476>.
34. Dolev, D.; Yao, A.C. On the Security of Public Key Protocols. *IEEE Trans. Inf. Theory* **1983**, *29*, 198–208.
35. Canetti, R.; Krawczyk, H. Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels. In *Proceedings of the Advances in Cryptology—EUROCRYPT 2001*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2001; Volume 2045, pp. 453–474.
36. 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, 2012; pp. 245–267.
37. Lata, K.; Cenkeramaddi, L.R. Fpga-based puf designs: A comprehensive review and comparative analysis. *Cryptography* **2023**, *7*, 55.
38. Karmakar, M.; Naz, S.F.; Shah, A.P. Fault-tolerant reversible logic gate-based RO-PUF design. *Mem.-Mater. Devices, Circuits Syst.* **2023**, *4*, 100055.
39. Gu, C.; Liu, W.; Cui, Y.; Hanley, N.; O'Neill, M.; Lombardi, F. A flip-flop based arbiter physical unclonable function (APUF) design with high entropy and uniqueness for FPGA implementation. *IEEE Trans. Emerg. Top. Comput.* **2019**, *9*, 1853–1866.

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