Abstract: Emerging as the effective strategy of intelligent transportation system (ITS), vehicular ad hoc networks (VANETs) have the capacity of drastically improving the driving experience and road safety. In typical VANET scenarios, high mobility and volatility of vehicles result in dynamic topology of vehicular networks. That is, individual vehicle may pass through the effective domain of multiple neighboring road-side-units (RSUs) during a comparatively short time interval. Hence, efficient and low-latency cross-domain verification with all the successive RSUs is of significance. Recently, a lot of research on VANET authentication and key distribution was presented, while the critical cross-domain authentication (CDA) issue has not been properly addressed. Particularly, the existing CDA solutions mainly reply on the acquired confidential keying information from the neighboring entities (RSUs and vehicles), while too much trustworthiness is granted to the involved RSUs. Please note that the RSUs are distributively located and may be compromised or disabled by adversary, thus vital vehicle information may be revealed. Furthermore, frequent data interactions between RSUs and cloud server are always the major requisite so as to achieve mutual authentication with cross-domain vehicles, which leads to heavy bandwidth consumption and high latency. In this paper, we address the above VANET cross-domain authentication issue under the novel RSU edge networks assumption. Please note that RSUs are assumed to be semi-trustworthy entity in our design, where critical vehicular keying messages remain secrecy. Homomorphic encryption design is applied for all involved RSUs and vehicles. In this way, successive RSUs could efficiently verify the cross-domain vehicle with the transited certificate from the neighbor RSUs and vehicle itself, while the identity and secrets of each vehicle is hidden all the time. Afterwards, dynamic updating towards the anonymous vehicle identity is conducted upon validation, where conditional privacy preserving is available. Moreover, pairing-free mutual authentication method is used for efficiency consideration. Formal security analysis is given, proving that the HCDA mechanism yields desirable security properties on VANET cross domain authentication issue. Performance discussions demonstrate efficiency of the proposed HCDA scheme compared with the state-of-the-art.

Keywords: Vehicular ad hoc networks (VANETs); homographic encryption; cross-domain authentication; dynamic key updating
innovative services and applications regarding transportation and traffic management, which is critical to populous metropolitan cities and regions. As the significant infrastructure of ITS, vehicle ad hoc network (VANET) is the self-organized and distributed wireless network built by heterogeneous vehicular entities including remote servers, road side units, and vehicles [4]. In general, VANET enables dynamic real-time communication for vehicles, thereby significantly enhances road safety and facilitate the driving experience.

In general, the basic components of VANET infrastructure consist of trusted authority (TA), road-side unit, and the terminal vehicles. As the top-level VANET management center and trustworthy key center, TA is in charge of crucial system operations including device registration, key generation, and vehicular data processing. Due to its keen demands for complex interactions and computation, currently TA applies advanced cloud computing technique for sufficient processing and storing capacities [5]. Please note that the distributed cloud servers are capable of arranging multiple VANET prototypes, which promote the construction of worldwide Internet of Vehicles (IoV) initiatives. Similarly, the promising 5G communicating infrastructure has been dedicated, thus stable and seamless data transmission can be guaranteed in this way.

The RSUs are organized as the distributed road-side facilities at fixed intervals, where their interacting ranges cover the entire road sections. Therefore, each vehicle can access the VANET through communication with its nearby RSU [6,7]. Specifically, the necessary key calculation and processing are performed in RSU side so as to provide low-latency data exchange with specific vehicles. This allows timely VANET applications delivery and sensitive vehicular data transmission. As mentioned above, in cloud-assisted VANET system, heterogeneous vehicular data are processed and stored in cloud server, while the novel edge architecture can be implemented so that low latency and high reliability properties of vehicle-to-RSU transmission (V2R) are satisfied accordingly [8]. In this case, instead of requesting information from the remote TA every time, the edge cluster including all the nearby RSUs is able to cache the frequently used data and manage the instant and frequent data exchange with vehicles, while the bandwidth burden for cloud server can be significantly alleviated [9–12].

The vehicles are the terminal users of VANET system, where massive vehicular data and road characteristics are collected [13–15]. Subsequently, the aggregated data are forwarded to cloud server for further analysis and management. The embedded on-board unit (OBU) in vehicle conduct packet transmission and reception in practical high-mobility VANET scenarios [16].

Two major type of VANET communications, including vehicle-to-RSU (V2R) communication, and vehicle-to-vehicle (V2V) communication, are enabled by the deployed dedicated short-range communication (DSRC) technique, which is an 802.11p-based wireless communication technology enable connection between vehicle and the surrounding entities in ITS. The inherent wireless transmission property leads to potential security risks and privacy threats in open environment [15,17]. The transmitted data may be forged or eavesdropped by malicious entities, bringing danger to the entire VANET and its vehicles. Consequently, effective authentication and verification mechanism should be deployed for security and privacy preservation [18,19].

Recently, lots of research has been done on VANET secure transmission. Various cryptographic techniques and safe strategies have been deployed in existing studies, where the proposed authentication and key management schemes have to a certain extent addressed the VANET security issues [20]. However, in practical VANET scenarios, high mobility and volatility of vehicles makes the authentication process challenging as the vehicles change their position fast. Numerous vehicles may continuously pass through effective domains of multiple RSUs in a short time interval. Moreover, random vehicle may join or leave the VANET network at any point of time beyond prediction [21,22]. For this concern, mutual authentication between each vehicle and all the RSU it passed by should be timely conducted prior to vehicular data exchange [23]. In other words, identity of the new vehicle will be verified whenever the vehicle enters the RSU effective domain, which is defined as cross-domain authentication. Considering the large number of participating
vehicles, huge time consumption and computation cost will be made for individual RSU, which crucially restricts the vast implementation of VANETs [13,24,25].

Presently, although some research attention has been paid so far, the critical cross-domain authentication issue has not been properly addressed in the field of VANET [11,26]. As a matter of fact, most of the existing mechanisms on VANET authentication tend to develop the verification scheme under static trust model, where only the occasion with initial RSU is discussed [27–29]. That is, the CDA occasion have not been taken into consideration at all. As for the rest schemes where CDA issue has been discussed indeed, all the successive RSUs have to inquire cloud server of confidential information, causing extra communication burden and high latency. In conclusion, trade-off between transmission security and efficiency in terms of cross-domain authentication issue remain unsolved [1]. Furthermore, in the existing CDA schemes, too much trustworthiness has been granted to the involving RSUs. Thus, vital vehicle information may be revealed, providing that certain RSU is compromised or disabled by adversary [30–33].

Motivated by the above discussion on VANET secure transmission, we address the above VANET CDA issue under the novel RSU edge networks assumption. In our design, the CDA issue can be solved by adopting the certificate transited from RSU clusters. In particular, the successive RSUs could efficiently verify the cross-domain vehicle with the transited certificate from the neighbor RSUs and vehicle itself, while the identity and secrets of each vehicle is hidden all the time. Please note that it is not necessary for the successive RSUs to exchange confidential information with remote cloud server, thus balance between efficiency and security is properly made. Meanwhile in our design, the dynamic updating towards the anonymous vehicle identity is conducted upon validation, where conditional privacy preserving is enabled in this way.

**Research Contributions**

In this paper, we develop a pairing-free homographic authentication and key management scheme for dynamic cross-domain authentication in VANETs. Our nontrivial efforts can be briefly summarized as follows:

- **Pairing-free certificateless mutual authentication scheme for cloud-assisted VANETs with edge computing infrastructure:** Our method adopts cloud-assisted system model with edge infrastructure. In our assumption, the massive vehicular data are to be transmitted and processed in remote cloud. Hence, practical requirements for sufficient processing and storing capacities can be satisfied. Meanwhile, the deployed edge RSU architecture enables low latency and high reliability of vehicle-to-RSU transmission (V2R), while the bandwidth burden for cloud server can be significantly alleviated. Furthermore, certificateless cryptography is exploited. TA and individual vehicle respectively generate the corresponding partial key pair so that the key escrow issue can be solved. The entire authentication scheme is performed without complex pairing functions so that the computation cost is drastically reduced.

- **Homographic key management towards cross-domain authentication:** In the proposed scheme, the cross-domain authentication issue is addressed by using the certificate transited from RSU clusters. Therefore, the successive RSUs could efficiently verify the cross-domain vehicle according to the certificate from the neighbor RSUs and vehicle itself. During the CDA process, homomorphic encryption is deployed for all participating RSUs and vehicles. Hence, RSU is able to conduct the verification process without accessing the vital vehicle secrets, where the vehicle privacy is guaranteed from the compromised RSUs. Please note that it is not necessary for the successive RSUs to exchange confidential information with remote cloud server, thus balance between efficiency and security is properly made.

- **Dynamic updating strategies on anonymous vehicle for conditional privacy preserving:** Constant identity is hidden during entire process, while the anonymous identities for RSUs and vehicles are constructed. Therefore, crucial security characteristics including unlinkability, conditional privacy-preserving, and user anonymity for all participating entities are provided.
Meanwhile, the transmitted vehicle certificate will be automatically updated whenever the vehicle passes by a new RSU. Thanks to the homographic encryption property and vehicle conditional privacy, confidential keying information cannot be extracted or forged by the compromised RSUs.

The remainder of this paper is organized as follows. Section 2 briefly introduces the related research progress. Section 3 illustrates the preliminary works for the reader to obtain a better understanding of the topic. Section 4 presents the proposed HCDA scheme in detail. Section 5 presents the security analysis. Section 6 displays the performance analysis. The final conclusions are drawn in Section 7.

2. Related Works

Currently, lots of research efforts on VANET secure transmission have been made [30,34]. Particularly, methods emphasizing on conditional-privacy preserving of the participating vehicles have been developed. In 2010, Zhang et al. [35] developed the decentralized group authentication protocol where each RSU organizes the vehicular group for users within its range. Hence, messages originating from the passing vehicles could be broadcast anonymously and verified by group members. False message sender could be revealed by the invoked third party. Similarly, the pseudonymous authentication protocol PACP is proposed [26], where the anonymous communication is guaranteed with the pseudonyms generated by both RSUs and vehicle. Later, Lu et al. [36] developed the dynamic key management scheme for VANET location-based services (LBSs). The LBS session is divided into various time slots with different session keys. In this way, the new session key can be autonomously updated. Afterwards, an identity-based VANET mutual authentication mechanism is designed by He et al. [37]. Bilinear pairing operations are not applied in the design so as to alleviate the computation cost. For the same purpose, Lo et al. developed the paring-free identity-based message authentication scheme with batch verification mechanism [38], thus optimized performance in term of time consumption can be achieved. Meanwhile, an anonymous mutual authentication protocol for VANETs is proposed [39], where group signature and batch message verification are adopted in multiple-vehicle scenarios. In 2019, Alazzawi et al. constructed a pseudo-identity-based message verification scheme [30] with resistance to insider attack and provision of message integrity. Please note that certificate revocation list is not deployed for the purpose of optimizing the communication cost.

Specifically, key management and vehicular data verification process for VANETs has been widely studied so far. In 2011, Hao et al. proposed a distributed key management framework with VANET group signature design [32]. Compromised RSUs and the colluding malicious vehicles can be timely detected and revoked. Meanwhile, the cooperative vehicular message authentication mechanism is used with the purpose of alleviating computation overhead. Hence, each vehicle only needs to perform a small amount of message verification tasks. Thereafter, another VANET message authentication mechanism EMAP [25] is developed by Wasef et al., where the time-consuming certificate revocation matching process is replaced with keyed hash-message-authentication-code (HMAC) design. Please note that the input key values are securely shared among on-board units of validated vehicles. Later, Chuang et al. [27] proposed a decentralized trust-extended message authentication mechanism TEAM for high-mobility V2V communication. The lightweight transitive trust relationships frame is deployed in order to reduce storage consumption. Meanwhile, emphasizing on low-latency computation for the certificate revocation procedure, Zhu et al. developed the hash-based VANET group signature [18], where cooperative message authentication among vehicular entities is implemented. Similarly, a two-factor lightweight VANETs authenticating schemes 2FLIP is proposed [13], which applied the decentralized certificate authority (CA) and biological password. Recently, multiple relevant VANETs key distribution and message validation methods have been proposed [2,8], where the blockchain structure is used for secure data sharing.

Due to the superiority in heterogenous data storing and parallel processing, cloud infrastructure has been extensively exploited in various VANET scenarios. In 2017, the vehicular message safe dissemination for cloud-assisted VANET-cellular heterogeneous network is studied in [9]. The message
delivery from remote server to destinated area is investigated. The proposed CMDS scheme provides reliable data sharing with the assistance of corresponding gateways and neighboring vehicles. Moreover, the resource allocation issue for vehicular cloud data is discussed by Lin et al. [40]. The legitimate RSUs help significantly improve the computing capability of vehicular cloud computing (VCC) system. In this way, optimal solution for VCC resource allocation is proposed under the modified semi-Markov decision process (SMDP) model. Furthermore, the message dissemination scheme for vehicular fog-assisted network is proposed by Ullah et al. [16], where message congestion avoidance is achieved. Thereafter, multiple methods on VANET secure transmission with cloud/fog infrastructure are accordingly presented [6,23,41].

As one of the critical issues in secure vehicular data transmission, cross-domain authentication under practical VANET environment has not been fully addressed so far. Presently, several relevant cross-domain solutions for other wireless transmission occasions have been proposed. In 2015, Li et al. proposed a certificateless cross-domain authentication and key management protocol for wireless mesh networks (WMNs) with multiple administrative domains [1]. The proposed CABA protocol enables two-round authenticated key agreement for the users affiliated to various WMN domains, while the discussion on high mobility and dynamic topology of WMN nodes is not included. Thereafter, He et al. developed the handshake scheme with symptom-matching for mobile healthcare social networks (MHSNs) [5]. Similarly, emphasizing on telemedicine communication system, a certificateless cross-domain authenticated asymmetric group key management is proposed [42], which provides resistance to key escrow problem. In 2019, a blockchain-assisted lightweight anonymous authentication scheme for vehicular fog service (VFS) is presented [4]. However, the proposed scheme mainly focuses on data sharing with vehicular data center, while efficient updating is not provided [26]. In conclusion, existing research either discussed the CDA issue in other general IoT wireless circumstances without taking into consideration the particular characteristics of VANET communications (e.g., high-mobility entities, self-organized topology, and instant data transmission), or failed to present the efficient and flexible security strategies employing extensive VANET infrastructures (e.g., cloud-assisted VANET, edge-based RSUs). As a result, the proposed scheme of this paper is of significance for practical VANETs.

3. Preliminaries

The essential cryptographic concepts and basic knowledge are introduced in this section for the purpose of facilitating the reader’s understanding. The definitions of elliptic curve cryptosystem (ECC), one-way hash function, and homomorphic encryption, have been respectively presented. Thereafter, the corresponding notations, system model, security requirements, and network assumptions are respectively described.

3.1. Elliptic Curve Cryptography (ECC)

Let \( p > 3 \) be the large prime, and \( \mathbb{F}_p \) be the finite field with order \( p \), where \( a, b \in \mathbb{F}_p \) satisfy \( 4a^3 + 27b^2 \mod p \neq 0 \). The elliptic curve \( E_p \( a, b \) \) over the finite field \( \mathbb{F}_p \) is defined with the following equation:

\[
y^2 = x^3 + ax + b \mod p,
\]

where \( (x,y) \in \mathbb{F}_p \). The addition operation on the curve is defined as point doubling when the two points are identical. Otherwise, it is defined as the point addition. All the points on the curve, as well as the point at infinity \( \infty \) form an additive Abelian group \( E(\mathbb{F}_p) \). Please note that \( \infty = (-\infty) \) performs as the identity element.
Definition 1 (Computational Diffie-Hellman Problem (CDHP)). Given $P, aP, bP \in \mathbb{G}_1$ for $a, b \in \mathbb{Z}_q^*$, where $P$ is a generator of $\mathbb{G}_1$, the advantage in computing $abP$ to solve the CDHP problem for any probabilistic polynomial-time (PPT) algorithm $A$ is negligible, which can be defined as:

$$\text{Adv}^{\text{CDHP}}_{A, \mathbb{G}_1} = \Pr[A (P, aP, bP) \rightarrow abP : a, b \in \mathbb{Z}_q^*].$$

Definition 2 (Elliptic Curve Discrete Logarithm Problem (ECDLP)). Given $P, Q \in \mathbb{G}_1$, where $Q = aP$. The advantage in finding the integer $a \in \mathbb{Z}_q^*$ in order to solve the ECDLP problem for any probabilistic polynomial-time (PPT) algorithm $A$ is negligible, which can be defined as:

$$\text{Adv}^{\text{ECDLP}}_{A, \mathbb{G}_1} = \Pr[A (P, aP) \rightarrow a : a \in \mathbb{Z}_q^*].$$

3.2. Hash Function

The one-way hash function $h(\cdot)$ is defined to be secure if the following properties can be achieved all:

1. Input a message $x$ of arbitrary length, it is easy to compute a message digest of a fixed length output $h(x)$.
2. Given $y$, it is hard to compute $x = h^{-1}(y)$.
3. Given $x$, it is computationally infeasible to find $x' = x$ such that $h(x') = h(x)$.

3.3. Homomorphic Encryption

The homomorphic encryption design allows the predefined standard computations on ciphertexts, with which the output matches the encryption result on the computations conducted on plaintexts. With its unique properties, homomorphic encryption can be widely applied into vast security designs and privacy preserving strategies. Hence, the transmitted data can be securely processed and out-sourced without revealing the privacy-related information. The encryption and decryption functionalities can be considered as the homomorphisms between plaintext and ciphertext spaces. In practical communication scenarios with semi-trusted entities, homomorphic encryption could remove privacy barriers inhibiting data sharing since the operations on encrypted data can be performed instead of direct calculations on the confidential user data. The Paillier cryptosystem is one of the homomorphic cryptosystems for public key infrastructure (PKI), the security of which is based on the decisional composite residuosity assumption (DCRA) described as follows:

Definition 3 (Decisional Composite Residuosity Assumption (DCRA)). Let $p, q$ be two large primes such that $n = pq$. Given $a \in \mathbb{Z}_n^*$, if there exist $\gamma \in \mathbb{Z}_n^2$ satisfying $a \equiv \gamma^n \mod n^2$, hence $a$ is defined as the $n$-th residue modulo $n^2$. Please note that given the composite $n$ and an integer $\beta$, it is hard to decide whether $\beta$ is the $n$-th residue modulo $n^2$. The Paillier encryption process is additively homomorphic. That is, the product of two ciphertexts will decrypt to the sum of their corresponding plaintexts. Let $m_1, m_2 \in \mathbb{Z}_n^*$ be the plaintexts, $r_1, r_2 < n$ be the random integers during encryption. The following additive homomorphic properties can be satisfied ($\Theta \in \mathbb{Z}_n^*$):

$$\begin{align*}
\text{Dec} \left( \text{Enc} \left( m_1, r_1 \right) \cdot \text{Enc} \left( m_2, r_2 \right) \mod n^2 \right) &= (m_1 + m_2) \mod n \\
\text{Dec} \left( \text{Enc} \left( m_1, r_1 \right)^\Theta \mod n^2 \right) &= (m_1 \Theta) \mod n
\end{align*}$$

where $\text{Enc} (\cdot), \text{Dec} (\cdot)$ denote the encrypting and decrypting operation, respectively.

3.4. Notations

The notations used in our scheme are listed in Table 1, along with the corresponding description.
Table 1. Notations.

| Symbol                  | Description                                      |
|-------------------------|--------------------------------------------------|
| VC, \{RSU_1, \cdots, RSU_n\} | Vehicular Cloud, Road-Side Units                  |
| \(G_1\)                | Cyclic Group                                    |
| \(P\)                  | Generator of \(G_1\)                            |
| \(ID_{T_i}, ID_{RSU_i}\) | Distinctive and Anonymous Identity for RSU_i     |
| \(\langle r_i^{RSU}, s_i^{RSU} \rangle\) | Partial Secret Key Pair of RSU_i                |
| \(\langle C_i, h_i \rangle\) | Encryption Key Pair of RSU_i                    |
| \(\langle A_i, \tilde{h}_i \rangle\) | Decryption Key Pair of RSU_i                    |
| \(M_j, N_j, S_j, T_j\) | Large Prime Values                              |
| \(ID_{V_i}, ID_{j}, ID_{k}^j\) | Distinctive and Anonymous Vehicle Identities |
| \(\langle k_j, r_j \rangle\) | Partial Secret Key Pair of Vehicle              |
| \(\langle Q_j, \xi_j \rangle\) | Encryption Key Pair of Vehicle                  |
| \(\langle \Gamma_j, \psi_j \rangle\) | Decryption Key Pair of Vehicle                  |
| \(\text{Proof}_{[j,k-1]}, \text{Proof}_{[j,k-1]}\) | Proofs in RSU\(_i\) Domain                    |
| \(\text{Credential}_{[j,k-1]}\) | Credential in RSU\(_k\) Domain                |
| \(sk_j\)               | Vehicle Session Key                             |
| \{TS_{1}, TS_{2}, TS_{3}, TS_{4}, TS_{5}\} | Timestamps                                      |
| \{V_1, \cdots, V_i\} | Vehicle Set                                     |
| \[\text{Enc}_{(C_i, A_i)}^{\tilde{h}_i}, \text{Dec}_{(C_i, A_i)}^{\tilde{h}_i}\] | Homomorphic Cryptography of RSU_i             |
| \[\text{Enc}_{\text{RSU}}^{(Q_i, \xi_i)}, \text{Dec}_{\text{RSU}}^{(Q_i, \xi_i)}\] | Homomorphic Cryptography of Vehicle            |

3.5. System Model

In this section, the used VANET infrastructure in our design is briefly illustrated. Please note that the deployed cloud-assisted VANET system with edge RSU layer could significantly satisfy the computing and storing requirements for massive vehicular data processing scenarios. As shown in Figure 1, the proposed VANET system model is composed of three different components with distinctive functionalities, which includes the cloud layer, edge layer, and device layer. Respectively, these three layers along with its general instructions are described as follows.

Cloud layer are considered as the core central data facilities responsible for the entire VANET system, where numerous vehicular data originating from terminal VANET devices are analyzed and safely stored. Moreover, crucial VANET system operations including device registration, confidential key generation, user verification, are all conducted by the topmost cloud layer, which is assumed to be valid and trustworthy at all time. Please note that the distributed cloud servers are capable of arranging multiple VANET prototypes, promoting the construction of worldwide Internet of Vehicles (IoV) initiatives. Similarly, the promising 5G communicating infrastructure has been dedicated, thus stable and seamless data transmission towards local RSUs can be guaranteed. For better description, we consider the entire cloud layer as one entity in our assumption.

Edge layer is a set of RSU clusters enabled by the direct and indirect wired connection between neighboring RSUs within certain vicinity. Instead of independently managing the data transmission tasks with in-range vehicles, each RSU cluster is able to collaboratively share essential vehicular information for vehicle authentication and then arrange distributive edge computation tasks.
Generally, in cloud-assisted VANET system, heterogeneous vehicular data are processed in cloud server, while the edge architecture can be deployed so that low latency and high reliability properties of vehicle-to-RSU transmission (V2R) are satisfied accordingly. In this case, instead of requesting information from the remote TA every time, the edge cluster including all the nearby RSUs is able to cache the frequently used data and manage the instant and frequent data exchange with vehicles, while the bandwidth burden for cloud server can be significantly alleviated. Practically, some RSUs located in harsh natural environment far away from the central server may be easily compromised or disabled. In this way, vital vehicle secret information should not be fully revealed to RSUs for user privacy preservation. In other words, the RSUs are assumed to be semi-trusted entities in our design.

Device layer refers to all the participating terminal vehicles, where heterogenous vehicular data and road information are aggregated. The embedded on-board unit in vehicle is responsible for transmission and reception in high-mobility VANET scenarios, while the deployed tamper-proof device (TPD) is for confidential message preserving. Hence, large amounts of temporary and high-speed V2V and V2R networks are constructed continuously. Due to resource restriction, the comparatively complex computation cannot be performed in vehicle side.

![Figure 1. VANET System Model.](image)

### 3.6. Networks Assumptions

As shown in Figure 1, the cloud layer and edge layer are correspondingly communicated through VANET core networks, which are constructed with wired connections between cloud server and local individual RSUs. Adequate safety strategies can be implemented accordingly, thus secure and reliable data transmissions are enabled. Consequently, data exchange in core networks are beyond our consideration. On the other hand, interactions between the edge layer and device layer are conducted through vehicle-to-RSU (V2R) communications performed by DSRC communicating technique. Moreover, the self-organized vehicle networks within the device layer are constructed through vehicle-to-vehicle (V2V) communications, while the inherent wireless transmission property of both V2R and V2V communication leads to potential security risks and privacy threats. The transmitted vehicular data may be forged or eavesdropped by malicious entities, bringing danger to the entire
VANET and its vehicles. Hence, proper security methods are of significance for safe wireless transmission of VANET.

3.7. Security Requirements

The design objective of our design is to enhance the security assurance of VANETs wireless transmissions, and to address the cross-domain authentication issue in practical VANETs. Moreover, efficiency for system management and authentication are to be taken into consideration. The following security requirements for VANET key management and authentication scheme should be fully satisfied.

- **Mutual Authentication:** In the VANET design, mutual authentication is the basic but leading security property ensuring that both VANET entities in one communication process authenticate each other. In this way, the impersonation attack towards certain device can be prevented.

- **Conditional Privacy Preserving:** As one of the essential privacy parameters, conditional privacy consists of user privacy protection and certain device retrieving. That is, the private information regarding user identity is safely preserved during the entire transmission process. Hence, the illegal tracing toward specific device cannot be performed. Resistance to replay attack is guaranteed as well. Meanwhile, the central server in charge of system management is able to reveal the real identity of individual vehicle if necessary. In this case, the compromised or corrupted vehicle can be timely revoked.

- **Non-repudiation:** The message sender of VANET cannot deny the authenticity of its signature on the transmitted messages. Non-repudiation ensures the validity of the transmitted information.

- **Unforgeability:** In wireless VANET transmission, adversary may selectively forge the valid certificates, keys, or signatures in order to pass the verification process and acquire crucial system secrets. Unforgeability against chosen message attack is the major property in secure data exchange.

- **Anonymity:** In open environment, the communication channels may be eavesdropped by malicious entities. Meanwhile, messages originating from the same device carry unique patterns in order for distinction in the receiver side. In this case, by analyzing the eavesdropped information, vital parameters such as sending frequency, user location may be exposed, which endangers user privacy. Hence, anonymity during the whole VANET communications is extremely important.

- **Session Key Establishment:** Upon verification, the shared session key between individual vehicle and VANET system should be established so as to provide safe data exchange. Due to the semi-trustworthiness of intermediate RSUs, the constructed session key should be hidden from the interacting RSUs.

4. The Proposed HCDA Scheme

In this section, the homographic authentication and key management scheme is presented, which emphasizes on dynamic cross-domain authentication issue in high-mobility VANET scenarios. In our design, the pairing-free certificateless cryptography is deployed for key escrow avoidance. Hence low-cost verification for resource-constrained wireless devices is achieved accordingly. User anonymity for both vehicles and RSUs is maintained during the entire processing time. Moreover, the independent anonymous identity updating mechanism is developed so as to prevent message linkability for individual vehicle of different RSU domains. Upon validation on each vehicle, the exclusive session key among cloud server and legitimate terminal user is constructed so as to facilitate independent data transmission. Thereafter, the cross-domain authentication issue is further discussed, where the successive RSUs could efficiently verify the vehicle from other RSU domain according to the confidential certificate from the neighboring RSUs. Particularly, the successive RSUs do not need to access the remote cloud server, thus drastically alleviate the bandwidth burden. In this way, a tradeoff between efficiency and security is properly made. Please note that homomorphic encryption
is deployed for CDA solution. Hence, RSU is able to conduct the verification process without accessing the vital vehicle secrets, where the vehicle privacy is guaranteed from the compromised RSUs.

Intuitively, the proposed scheme can be roughly divided into device registration, mutual authentication, and cross-domain authentication strategy. In device registration section, the nontrivial system initialization are preliminarily performed. Registration process towards all the participating vehicles and RSUs are conducted. In this way, vital private information including fundamental vehicle identity and initial secret key are safely stored in cloud server. Subsequently, the mutual authentication process regarding vehicle and initial RSU is performed in mutual authentication section, where the new vehicle is able to participate in VANET system after validation with cloud server. The independent secret key is generated for each vehicle. Finally, the solution towards cross-domain authentication issue is presented. The authentication mechanism with random approaching vehicle is provided in RSU side, while the edge RSU network is used for confidential key sharing. In this way, the detailed routine information for each legitimate vehicle can be effectively monitored and organized by cloud server, which is essential for location-related VANET applications including navigation, remote surveillance, and traffic dispute settlement.

4.1. Device Registration

The device registration operation is conducted for system initialization and vehicle registration. As mentioned above, the vehicular cloud (VC) is assumed to be validated and trustworthy entity during the whole communication session. Hence, vital VANET parameters are generated and allocated from VC to destined devices. Initially, $\mathbb{G}_1$ is defined as the cyclic group generated by large prime order $q$, where $P$ denotes the generator of $\mathbb{G}_1$. Meanwhile, the secure cryptographic hash functions $H_1, H_2, H_3, H_4, H_5, h_1, h_2, h_3, h_4$ are respectively performed as

\[
\begin{align*}
H_1 : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* & \rightarrow \mathbb{Z}_q^* \\
H_2 : \{0,1\}^* \times \{0,1\}^* \times \mathbb{G}_1 & \rightarrow \mathbb{Z}_q^* \\
H_3 : \{0,1\}^* \times \{0,1\}^* \times \mathbb{G}_1 \times \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* & \rightarrow \mathbb{Z}_q^* \\
H_4 : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* & \rightarrow \mathbb{Z}_q^* \\
H_5 : \mathbb{G}_1 & \rightarrow \mathbb{Z}_q^* \\
h_1 : \{0,1\}^* \times \{0,1\}^* \times \mathbb{G}_1 & \rightarrow \mathbb{Z}_q^* \\
h_2 : \{0,1\}^* \times \mathbb{G}_1 & \rightarrow \mathbb{Z}_q^* \\
h_3 : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* & \rightarrow \mathbb{Z}_q^* \\
h_4 : \{0,1\}^* & \rightarrow \mathbb{Z}_q^*
\end{align*}
\]

Accordingly, the system parameter set $\text{param} = \{\mathbb{G}_1, q, P, H_1, H_2, H_3, H_4, H_5, h_1, h_2, h_3, h_4\}$ are published.

Respectively, the unique identity $ID^i_\ell \in \{0,1\}^*$ for each legitimate RSU is issued. The correlated secret $s^i_{\text{RSU}} \in \mathbb{Z}_q^*$ is randomly generated for independent RSU. Therefore, the confidential RSU information set $\langle ID^i_\ell, s^i_{\text{RSU}} \rangle$ is safely shared among VC and RSU itself. Similarly, it is prerequisite for all the vehicles to register in advance. The distinctive vehicle identity $ID^j_v \in \{0,1\}^*$ is distributed, along with the secret key $k_j \in \mathbb{Z}_q^*$ generated by VC. Hence the key pair for vehicle is $\langle ID^j_v, k_j \rangle$. Please note that the whole device registration is safely performed in offline mode. Crucial vehicular personal information regarding user name, address, social identifier, and phone number, are recorded in VC as well. Consequently, VC constructs the unique vehicular records regarding all registered vehicles and RSUs as shown in Table 2.
Table 2. Vehicular Records for Registered Entities.

| Number | Type | Distinctive Identity | Assigned Secret | Location | Name/Add./Social ID/Phone No. |
|--------|------|----------------------|-----------------|----------|-----------------------------|
| 1      | RSU  | ID\textsubscript{RSU}\textsuperscript{1} | s\textsubscript{RSU}\textsuperscript{1} | √        | \                           |
| 2      | RSU  | ID\textsubscript{RSU}\textsuperscript{2} | s\textsubscript{RSU}\textsuperscript{2} | √        | \                           |
| ...    | ...  | ...                  | ...             | ...      | ...                         |
| i      | RSU  | ID\textsubscript{RSU}\textsuperscript{i} | s\textsubscript{RSU}\textsuperscript{i} | √        | \                           |
| 1      | Vehicle | ID\textsubscript{V}\textsuperscript{1} | k\textsubscript{1} | \         | √                           |
| 2      | Vehicle | ID\textsubscript{V}\textsuperscript{2} | k\textsubscript{2} | \         | √                           |
| ...    | ...  | ...                  | ...             | ...      | ...                         |
| j      | Vehicle | ID\textsubscript{V}\textsuperscript{j} | k\textsubscript{j} | \         | √                           |

For anonymity protection, the registered RSU randomly generates \( r\textsubscript{RSU}\textsuperscript{i} \in \mathbb{Z}_q^* \) and periodically extracts the current RSU anonymous identity \( ID\textsubscript{RSU}\textsuperscript{i} \) as

\[
ID\textsubscript{RSU}\textsuperscript{i} = h_1 \left( T S\textsubscript{i}, ID\textsubscript{RSU}\textsuperscript{i}, r\textsubscript{RSU}\textsuperscript{i} \right),
\]  

where the current timestamp \( T S\textsubscript{i} \) is adopted for freshness assurance. In this case, each RSU session identity \( D\textsubscript{RSU}\textsuperscript{i} \) is only valid within certain time period. The RSU partial secret key pair \( \langle r\textsubscript{RSU}\textsuperscript{i}, s\textsubscript{RSU}\textsuperscript{i} \rangle \) is then stored in RSU side, while \( r\textsubscript{RSU}\textsuperscript{i} \) is kept secret to \( VC \).

In the next, the homomorphic encryption infrastructure for each registered RSU is constructed. RSU independently chooses two large prime value \( M_i \) and \( N_i \) with \( \text{gcd}(M_i, N_i, (M_i - 1) (N_i - 1)) = 1 \). Hence, the calculations on \( O_i \) and \( \Lambda_i \) can be performed as

\[
\begin{align*}
O_i &= M_i N_i \\
\Lambda_i &= \text{lcm}(M_i - 1, N_i - 1)
\end{align*}
\]  

Thereafter, RSU selects random \( h_i \in \mathbb{Z}_{O_i}^* \) and computes

\[
\bar{h}_i = \ell_i \left( h_i^{\Lambda_i} \mod O_i \right) \mod O_i,
\]  

where the function \( \ell_i(x) = \frac{x^{O_i - 1}}{O_i} \). At this point, the encryption key pair for RSU is extracted as \( \langle O_i, h_i \rangle \).

Subsequently, RSU performs the following calculations:

\[
\begin{align*}
\mathcal{R}^i &= r\textsubscript{RSU}\textsuperscript{i} P \\
\text{Cert}^i_{RSU} &= H_1 \left( T S\textsubscript{2}, ID\textsubscript{RSU}\textsuperscript{i}, O_i, h_i, \mathcal{R}^i \right)
\end{align*}
\]  

where \( T S\textsubscript{2} \) denotes the latest timestamp. At this point, the RSU parameters set denoted as \( \langle T S\textsubscript{2}, ID\textsubscript{RSU}\textsuperscript{i}, O_i, h_i, \mathcal{R}^i, \text{Cert}^i_{RSU} \rangle \) is periodically broadcast to all entities within its effective domain.

4.2. Mutual Authentication

In this section, mutual authentication between vehicle and VANET system is conducted. Initially, assuming the vehicle of identity \( ID\textsubscript{V} \), partial secret key \( k_j \) is approaching specific RSU, vehicle itself randomly generates its own secret \( r_j \in \mathbb{Z}_q^* \). At this point, partial secret \( \langle k_j, r_j \rangle \) is stored by vehicle. Consequently, the anonymous identity used in the authentication session is computed as

\[
ID_j = h_2 \left( ID\textsubscript{V}, r_j P \right),
\]
At the same time, vehicle is acknowledged of the published RSU parameters set \( \langle TS_j^1, ID_{RSU}^j, O_i, h_i, R_i^j, Cert_{RSU}^j \rangle \). Upon extracting the parameters, freshness verification towards the timestamp \( TS_j^2 \) is first carried out by checking whether \( |TS_j^{cur} - TS_j^2| \leq \varepsilon_1 \) holds, where \( TS_j^{cur} \) indicates the current timestamp. Subsequently, by validating the certificate \( Cert_{RSU}^j \), integrity of the received message can be guaranteed. Upon validation, the encryption key pair \( \langle O_i, h_i \rangle \) can be extracted by vehicle. Similarly, the homomorphic encryption design for vehicle is constructed. The vehicle with identity \( ID_i \) then chooses two large prime value \( \{ S_j, T_j \} \) with gcd \( (S_jT_j, (S_j - 1)(T_j - 1)) = 1 \). Hence, the calculations on \( Q_j, \Gamma_j \) can be performed as

\[
\begin{aligned}
Q_j &= S_jT_j \\
\Gamma_j &= \text{lcm}(S_j - 1, T_j - 1).
\end{aligned}
\]

Thereafter, vehicle selects random \( \xi_j \in \mathbb{Z}_{Q_j}^\ast \) and computes

\[
\nu_j = \phi_j \left( \xi_j^r \mod Q_j \right) \mod Q_j,
\]

where the function \( \phi_j(y) = \frac{y-1}{Q_j} \).

At this point, the encryption key pair for vehicle is extracted as \( \langle Q_j, \xi_j \rangle \). The vehicle then uses the randomly generated secret key \( r_j \) and the acquired RSU encryption key pair \( \langle O_i, h_i \rangle \) to perform the encrypting operations as

\[
\begin{aligned}
\eta_j &= H_2 \left( TS_j^3, ID_j, k_j, r_j, P \right) \\
\zeta_j &= H_3 \left( TS_j^3, ID_j, R_i^j, Q_j, \xi_j, \eta_j \right) \\
Y_j &= r_jR_i^j \\
Cert_{V}^j &= \text{Enc}_{\langle O_i, h_i \rangle}^{r_j} \left[ \eta_j \| Q_j \| \xi_j \| \zeta_j \right].
\end{aligned}
\]

Please note that \( \text{Enc}_{\langle O_i, h_i \rangle}^{r_j} [M] \) denotes the homomorphic encryption performed as

\[
\text{Enc}_{\langle O_i, h_i \rangle}^{r_j} [M] = H_i^M \cdot r_j^O_i \mod O_i^2.
\]

Thereafter, vehicle sends the following requesting packet

\[
\langle \text{Request}, TS_j^3, ID_j, Y_j, Cert_{V}^j \rangle
\]

to RSU for further validation.

On the receipt of the verification packet, freshness verification towards timestamp \( TS_j^3 \) is first carried out by checking whether \( |TS_j^{cur} - TS_j^3| \leq \varepsilon_2 \) holds, where \( TS_j^{cur} \) indicates the current timestamp. Subsequently, RSU is able to decrypt the received \( Cert_{V}^j \) by computing

\[
\begin{aligned}
\langle \eta_j \| Q_j \| \xi_j \| \zeta_j \rangle &= \text{Dec}_{\langle O_i, h_i \rangle}^{\eta_j} \left[ Cert_V^j \right] \\
&= \ell_i \left( \left[ Cert_V^j \right] \Lambda_i \mod O_i^2 \right) \\
&= \frac{\ell_i \left( \left[ Cert_V^j \right] \Lambda_i \mod O_i^2 \right)}{\Lambda_i} \mod O_i,
\end{aligned}
\]

where \( \text{Dec}_{\langle O_i, h_i \rangle}^{\eta_j} [C] \) denotes the RSU homomorphic decryption performed as

\[
\begin{aligned}
\text{Dec}_{\langle O_i, h_i \rangle}^{\eta_j} [C] &= \frac{\ell_i \left( C \Lambda_i \mod O_i^2 \right)}{\Lambda_i} \mod O_i.
\end{aligned}
\]
Please note that the mathematical correctness for the above decryption can be briefly illustrated as

$$\begin{align*}
\text{Dec}^{\mathcal{O}_i}_{\Pi_i, \mathcal{A}_i} \left[ \text{Enc}^{r_i}_{\mathcal{O}_i, \mathcal{A}_i} [M] \right]
&= \ell_i \left( \frac{\left[ \text{Enc}^{r_i}_{\mathcal{O}_i, \mathcal{A}_i} [M] \right]^{\mathcal{A}_i} \mod \mathcal{O}_i^2}{\bar{a}_i} \right) \mod \mathcal{O}_i \\
&= \ell_i \left( \left[ h_i^M \cdot r_i \mod \mathcal{O}_j^2 \right]^{\mathcal{A}_i} \mod \mathcal{O}_i \right) \mod \mathcal{O}_i \\
&= M \mod \mathcal{O}_j
\end{align*}$$

Hence, $\langle n_j || Q_j, \xi_j || \mathcal{A}_j \rangle$ is successfully extracted from $\text{Cert}_j$ by RSU. Confidentiality of the information can be verified by checking the value of $\mathcal{A}_j$ according to the currently acquired $n_j$ and the previously broadcast $\mathcal{R}^j$ from RSU. If validated, RSU accepts the vehicle homomorphic encryption key pair $(Q_j, \xi_j)$. Moreover, with the stored $\mathcal{R}^j = r^j_{\text{RSU}} \xi^j_{\text{RSU}} P$ and $Y_j = r_j \mathcal{R}^j$, the following $\Psi_j$ can be calculated as

$$\begin{align*}
\Psi_j
&= \left( r^j_{\text{RSU}} \xi^j_{\text{RSU}} \right)^{-1} Y_j \\
&= r_j \left( r^j_{\text{RSU}} \xi^j_{\text{RSU}} \right)^{-1} \mathcal{R}^j \\
&= r_j \left( r^j_{\text{RSU}} \xi^j_{\text{RSU}} \right)^{-1} \left( r^j_{\text{RSU}} \xi^j_{\text{RSU}} \right) P \\
&= r_j P
\end{align*}$$

At this point, RSU uploads $\langle TS^j_4, ID_j, \Psi_j, n_j \rangle$ to $\text{VC}$ for remote identification. As mentioned above, the identity information $\langle ID_j, k_j \rangle$ involving the legitimate vehicles are stored in $\text{VC}$ database. Hence, $\text{VC}$ is able to confirm the corresponding vehicle identity $ID_j$ with the transmitted $\langle TS^j_4, ID_j, \Psi_j, n_j \rangle$ from RSU. If matches, identity of certain vehicle is verified. The vehicle access to VANET system can be granted by $\text{VC}$.

Thereafter, $\text{VC}$ computes $\omega_j = h_2 \left( ID_j, k_j, r_j P \right)$ and replies to RSU with the acknowledgement message $\langle \text{ack}, ID_j, \omega_j \rangle$. Upon receipt of the acknowledgement message, RSU update the vehicle identity as $ID_j = h_2 \left( ID_j, r^j_{\text{RSU}} \xi^j_{\text{RSU}} P \right)$, where the RSU key pair $(r^j_{\text{RSU}} \xi^j_{\text{RSU}})$ is adopted. Please note that in our design, anonymous identity of the participating vehicle is safely updated as soon as a successful verifying session is operated. In this case, the message unlinkability for different communication sessions can be guaranteed. Untraceability of specific vehicle is preserved as well.

In the next, RSU conducts the vehicle homomorphic encryption process with the aforementioned vehicle key pair $(Q_j, \xi_j)$ and its own $r^j_{\text{RSU}}$ as

\[
\begin{cases}
\text{Cert}^j_{\text{RSU}} = \text{Enc}^r_{\mathcal{O}_j, \mathcal{A}_j} [\omega_j] \\
\Phi_j = H_4 \left( TS^j_4, ID^j_4, \text{Cert}^j_{\text{RSU}} \right)
\end{cases}
\]

Please note that $\text{Enc}^r_{\mathcal{O}_j, \mathcal{A}_j} [M]$ denotes the homomorphic encryption performed as

\[
\text{Enc}^r_{\mathcal{O}_j, \mathcal{A}_j} [M] = \xi_j^M \cdot (r^j_{\text{RSU}})^Q_j \mod \mathcal{O}_j^2.
\]

Hence, RSU is able to broadcast the packet $\langle TS^j_4, ID^j_4, \text{Cert}^j_{\text{RSU}}, \Phi_j \rangle$ to the destination vehicle.
Upon receipt of the packet, freshness verification towards the timestamp $TS^i_{cur}$ is first carried out by checking whether $|TS^i_{cur} - TS^i_4| \leq \epsilon^3$ holds, where $TS^i_{cur}$ indicates the current timestamp. Subsequently, vehicle is able to decrypt the received $Cert^i_{RSU}$ by computing

$$\omega_j = \frac{Dec^{(Q,\Gamma)}_{j} [Cert^i_{RSU}]}{\phi_j \left(\left[Cert^i_{RSU}\right]^{T_j} \mod Q^2_j\right)} \mod Q,$$

(18)

where $Dec^{(Q,\Gamma)}_{j} [\cdot]$ denotes the vehicle homomorphic decryption performed as

$$Dec^{(Q,\Gamma)}_{j} [C] = \frac{\phi_j \left(C^{T_j} \mod Q^2_j\right)}{\psi_j} \mod Q.$$

(19)

Please note that the mathematical correctness for the above decryption can be briefly illustrated as

$$\begin{align*}
Dec^{(Q,\Gamma)}_{j} \left[ Enc^{r^i_{RSU}}_{(Q,\Gamma_j)} [M] \right] &= \frac{\phi_j \left[ Enc^{r^i_{RSU}}_{(Q,\Gamma_j)} [M] \right]^{T_j} \mod Q^2_j}{\psi_j} \mod Q_j \\
&= \frac{\phi_j \left(s^{r^i_{RSU}}_j \cdot \left(r^i_{RSU}\right)^{\Gamma_j} \mod Q^2_j \right)^{T_j} \mod Q^2_j}{\phi_j \left(s^{r^i_{RSU}}_j \mod Q^2_j\right)} \mod Q_j \\
&= M \mod Q_j.
\end{align*}$$

(20)

Hence, $\omega_j$ is successfully extracted from $Cert^i_{RSU}$ by vehicle. Confidentiality of the delivered packet can be verified by checking the value of $\Phi_j$. If validated, vehicle conducts the final authentication on $\omega_j = h_2 \left(ID^j, k_j r_j P\right)$.

At this point, mutual authentication for vehicle and RSU is completed, which adopts homomorphic encryption and certificateless cryptographic technique. The semi-trusted RSUs can proceed the authentication process without acquiring confidential secrets for specific vehicle. Meanwhile, the partial secret keys of individual vehicle are respectively generated by $VC$ and vehicle itself. The complex pairing operations are not used in our design, providing new prospect for resource-limited VAENTs devices. The session key established between $VC$ and vehicle is calculated as $sk_j = H_5 (k_j r_j P)$, which is used as the unique identifying code shared between vehicle and $VC$. Meanwhile, the secure vehicular data exchange is performed through the aforementioned homomorphic cryptographic techniques including $\left[ Enc^{r^i_{RSU}}_{(Q,\Gamma_j)}, Dec^{\phi_j}_{(Q,\Gamma_j)} \right]$, and $\left[ Enc^{r^i_{RSU}}_{(Q,\Gamma_j)}, Dec^{\phi_j}_{(Q,\Gamma_j)} \right]$.

### 4.3 Cross-Domain Authentication Strategy

In this section, the specific cross-domain authentication problem in high-mobility VANET is further investigated. Generally, in practical VANET scenarios, individual vehicles randomly pass through effective domains of multiple RSUs within short time intervals. Hence, temporary and volatile data transmission and dynamic network topologies are enabled. Moreover, crucial vehicular operations for independent vehicle, such as key updating, identification, and revocation may be conducted at any
time. Efficient authentication mechanism between vehicle and all the encountering RSUs is required whenever the vehicle enters the RSU effective domain. Consequently, secure and reliable VANET transmissions can be achieved. Considering the large number of participating vehicles, huge time consumption and computation cost will be made for individual RSU, which crucially restricts the vast implementation of VANETs. As shown in Figure 2, vehicle $V_i$ has successfully passed the mutual authentication process with certain RSU$_1$ at timepoint $t_1$, where the interaction with VC is performed for confidential key information. Subsequently, at $t_2$ ($t_2 > t_1$), dynamic verification should be conducted as soon as $V_i$ approaches the effective domain of a brand-new RSU$_2$. Please note that the mutual trustworthiness of $V_i$ ↔ RSU$_2$ is constructed in this way. On further timepoint $t_n$ ($t_n > t_{n-1}$), dynamic cross-domain authentication with random RSU$_n$ should also be conducted.

![Figure 2. Cross-Domain Authentication in VANETs.](image)

To address the CDA issue, our design adopts the novel communication workflow, which could significantly avoid heavy bandwidth burden of VC for cross-domain authentication. The workflow logic can be briefly elaborated in Figure 3, where certain vehicle set $\{V_1, \cdots, V_i\}$ is assumed to respectively carry out linear validation with the encountering RSU set $\{\text{RSU}_1, \cdots, \text{RSU}_n\}$. Please note that the vehicles are assumed to follow the same path RSU$_1 \rightarrow$ RSU$_n$ for better description. In this case, the vehicle in $\{V_1, \cdots, V_i\}$ conducts initial authentication with RSU$_1$, where the detailed verification and key management process has been illustrated previously. Please note that in this phase data acquisition from remote VC is enabled for each vehicle of $\{V_1, \cdots, V_i\}$. Thereafter, vital certificate information is delivered to the successive RSU$_2$ such that efficient validation between RSU$_2$ and each vehicle can be achieved. The validation process does not require remote assistance of VC from now on, while fast and efficient verification is provided. Furthermore, the anonymous identity is dynamically updated upon each verification. The detailed CDA solution is presented as follows.
Figure 3. Workflow of CDA Solution in VANETs.

According to the authentication and key management scheme in the previous section, mutual authentication with the initial RSU can be successfully finished after vehicle itself validates the delivered packet $\langle TS^j, ID^j, Cert^{RSU}_j, \Phi^j \rangle$ from RSU. The secure vehicular data exchange is performed through the homomorphic cryptographic techniques including $[\text{Enc}^j_{\langle O^j, h^j \rangle}, \text{Dec}^j_{\langle O^j, h^j \rangle}]$, and $[\text{Enc}^j_{\langle Q^j, \xi^j \rangle}, \text{Dec}^j_{\langle Q^j, \xi^j \rangle}]$. In our CDA solution, RSU is designed to use the edge RSU networks to achieve fast and efficient validation without accessing the remote VC. That is, RSU calculates the original vehicular proof as

$$\text{Proof}^j_{\langle i, 1 \rangle} = \text{Cert}^{RSU}_j \cdot \text{Enc}^j_{\langle Q^j, \xi^j \rangle} \left[ h_2 \left( ID^j_{RSU}, Y^j \right) \right],$$

(21)

where $r^j_{RSU} \in Z_q^*$ is the newly generated pseudorandom for CDA mechanism and $r^j_{RSU} \neq r^j_{RSU}$. That is, the $\text{Proof}^j_{\langle i, 1 \rangle}$ is constructed by two different pseudorandom $r^j_{RSU}$ and $r^j_{RSU}$. Moreover, the relevant certificate is computed as

$$\text{Cert}^{CDA}_{\langle i, 1 \rangle} = h_3 \left( ID^j, Q^j, \xi^j, \text{Proof}^j_{\langle i, 1 \rangle} \right).$$

(22)

In this case, the initial RSU will simultaneously broadcast the packet $\langle ID^j, Q^j, \xi^j, \text{Proof}^j_{\langle i, 1 \rangle}, \text{Cert}^{CDA}_{\langle i, 1 \rangle} \rangle$ to all its neighboring RSUs through wired edge networks. On receiving the packet, all its neighboring RSUs temporarily store it in their storage for possible further use. If not required in certain time interval $\Lambda_{CDA}$, the packet is abandoned.

According to the previous assumption on vehicle path $\text{RSU}_1 \rightarrow \text{RSU}_n$, vehicle is approaching the effective domain of $\text{RSU}_2$ on timepoint $t_2$, while the RSU parameters set $\langle TS^j \rightarrow ID^j_{RSU}, O_2, h^2, R^2, \text{Cert}^{RSU}_2 \rangle$ is periodically broadcast by $\text{RSU}_2$ (index $i \leftarrow 2$). At this moment, vehicle generates the new random number $r^CDA_i \in Z_q^*$ and calculates the corresponding proof and credential as

$$\begin{cases} 
\text{Proof}^CDA_{\langle i, 1 \rangle} = \text{Enc}^CDA_{\langle Q^j, \xi^j \rangle} \left[ \omega_j - h_2 \left( ID^j_{RSU}, Y^j \right) \right] \\
\text{Credential}^CDA_{\langle i, 1 \rangle} = h_4 \left( \text{Enc}^CDA_{\langle Q^j, \xi^j \rangle} \left[ 2\omega_j \right] \right). 
\end{cases}$$

(23)

Subsequently, vehicle conducts the RSU encryption using the broadcast key $\{O_2, h_2\}$ of $\text{RSU}_2$ as

$$\text{Cert}^{FA}_{\langle i, 1 \rangle} = \text{Enc}^CDA_{\langle O^j_2, h^j_2 \rangle} \left[ ID^j, r^CDA_i, \text{Proof}^CDA_{\langle i, 1 \rangle}, \text{Credential}^CDA_{\langle i, 1 \rangle} \right].$$

(24)
which will be delivered to RSU$_2$ as the fast authentication packet in the form of $\langle \text{Fast}_\text{Auth}, \text{Cert}^{\text{FA}}_{[j,1]} \rangle$.

On receiving $\langle \text{Fast}_\text{Auth}, \text{Cert}^{\text{FA}}_{[j,1]} \rangle$, RSU$_2$ is able to decrypt the received $\text{Cert}^{\text{FA}}_{[j,1]}$ according to

$$
\text{Dec}_{(Q_2,\delta_2)}^{\text{FA}} \left[ \text{Cert}^{\text{FA}}_{[j,1]} \right] = \text{Dec}_{(Q_2,\delta_2)}^{\text{FA}} \left[ \text{Enc}_{(Q_2,\delta_2)}^{\text{CDA}} \left[ \left( ID_j^1, r^{\text{CDA}}_j P, \text{Proof}^{-}_r, \text{Credential}_{[j,1]} \right) \right] \right].
$$

(25)

Consequently, vehicle identity $ID_j^1$ is detected by RSU$_2$. As mentioned above, the certificate information of vehicle has already broadcast to all neighboring RSUs including RSU$_2$. That is, RSU$_2$ has already stored $\langle ID_j^1, Q_j, \xi_j, \text{Proof}^{-}_r, \text{Cert}^{\text{CDA}}_{[j,1]} \rangle$ in its storage within certain time interval $\Delta_{\text{CDA}}$. If $ID_j^1$ matches, RSU$_2$ extracts $\text{Proof}^{-}_r$ from the stored packet and $\langle \text{Proof}^{-}_r, \text{Credential}_{[j,1]} \rangle$ from the fast authentication packet. The validation on

$$h_4 \left( \text{Proof}^{-}_r, \text{Proof}_{[j,1]} \right) \triangleq \text{Credential}_{[j,1]}$$

(26)

is performed in this case. If Equation (26) holds, the requesting vehicle is successfully verified by RSU$_2$. Please note that the correctness can be elaborated as follows

L.H.S.

$$= h_4 \left( \text{Proof}^{-}_r \cdot \text{Proof}_{[j,1]} \right)
= h_4 \left( \text{Cert}^{\text{FA}}_{RSU} \cdot \text{Enc}_{(Q_2,\delta_2)}^{\text{RSU}} \left[ h_2 \left( ID_{\text{RSU}}^1, Y_j \right) \right] \cdot \text{Enc}_{(Q_2,\delta_2)}^{\text{CDA}} \left[ \omega_j \cdot h_2 \left( ID_{\text{RSU}}^1, Y_j \right) \right] \right)
= h_4 \left( \text{Enc}_{(Q_2,\delta_2)}^{\text{RSU}} \left[ \omega_j \right] \cdot \text{Enc}_{(Q_2,\delta_2)}^{\text{RSU}} \left[ h_2 \left( ID_{\text{RSU}}^1, Y_j \right) \right] \right) \cdot \text{Enc}_{(Q_2,\delta_2)}^{\text{CDA}} \left[ \omega_j \right]
= h_4 \left( \text{Enc}_{(Q_2,\delta_2)}^{\text{RSU}} \left[ \omega_j \right] \cdot \text{Enc}_{(Q_2,\delta_2)}^{\text{CDA}} \left[ \omega_j \right] \right)
= \text{Credential}_{[j,1]}.$$

(27)

R.H.S.

$$= \text{Credential}_{[j,1]}
= h_4 \left( \text{Enc}_{(Q_2,\delta_2)}^{\text{CDA}} \left[ 2\omega_j \right] \right)
= h_4 \left( \text{Enc}_{(Q_2,\delta_2)}^{\text{CDA}} \left[ \omega_j \right] \cdot \text{Enc}_{(Q_2,\delta_2)}^{\text{CDA}} \left[ \omega_j \right] \right).
$$

(28)

With $\text{Enc}_{(Q_2,\delta_2)}^{\text{RSU}} \left[ \omega_j \right] = \text{Enc}_{(Q_2,\delta_2)}^{\text{CDA}} \left[ \omega_j \right]$, L.H.S. = R.H.S. holds. Hence, the correctness of $h_4 \left( \text{Proof}^{-}_r \cdot \text{Proof}_{[j,1]} \right) = \text{Credential}_{[j,1]}$ is proved. At this point, the previous stored vehicle homomorphic encryption key pair $\langle Q_j, \xi_j \rangle$ can be used by RSU$_2$. The secure vehicular data exchange is performed through the homomorphic cryptographic techniques including $\left[ \text{Enc}_{(Q_2,\delta_2)}^{\text{CDA}}, \text{Dec}_{(Q_2,\delta_2)}^{\text{RSU}} \right]$, and $\left[ \text{Enc}_{(Q_2,\delta_2)}^{\text{RSU}}, \text{Dec}_{(Q_2,\delta_2)}^{\text{CDA}} \right]$. 

---

Symmetry 2020, 12, 1003
In this case, RSU₂ computes the certificate information for final authentication in vehicle side, which is encrypted with vehicle homomorphic encryption key pair \(\langle Q_i, \xi_i\rangle\) and the generated pseudorandom \(r^\text{RSU}_i \in \mathbb{Z}_q^*\) as

\[
\text{Cert}_{\text{Final}}^2 = \text{Enc}_{\langle Q_i, \xi_i\rangle}^{\text{RSU}} [\text{Proof}^\gamma_{\text{Final}}^{\text{RSU}} | \text{Proof}^\gamma_{\text{Final}}^{\text{RSU}} | H_4 \left( TS^2_{\text{CDA}}, ID^2_j, \text{Proof}^\gamma_{\text{Final}}^{\text{RSU}} \right)],
\]  

(29)

where \(TS^2_{\text{CDA}}\) is the current timestamp for cross-domain authentication. The packet \(\langle TS^2_{\text{CDA}}, ID^2_j, \text{Cert}_{\text{Final}}^2\rangle\) is then sent to vehicle for mutual verification.

On receiving \(\langle TS^2_{\text{CDA}}, ID^2_j, \text{Cert}_{\text{Final}}^2\rangle\), freshness verification towards the timestamp \(TS^2_{\text{CDA}}\) is carried out by checking whether \(|TS^2_{\text{CDA}} - TS^2_{\text{CDA}}| \leq \epsilon_3\) holds, where \(TS^2_{\text{CDA}}\) indicates the current timestamp. Subsequently, vehicle is able to decrypt the received \(\text{Cert}_{\text{Final}}^2\) by computing

\[
\begin{align*}
\text{Dec}_{\langle Q_i, \xi_i\rangle}^{\langle Q_j, \xi_j\rangle} [\text{Cert}_{\text{Final}}^2] &= \frac{\phi_j \left( [\text{Cert}_{\text{Final}}^2]^{\xi_j} \mod Q_j \right)}{\phi_j} \mod Q_j \\
&= \text{Proof}^\gamma_{\text{Final}}^{\text{RSU}} | \text{Proof}^\gamma_{\text{Final}}^{\text{RSU}} | H_4 \left( TS^2_{\text{CDA}}, ID^2_j, \text{Proof}^\gamma_{\text{Final}}^{\text{RSU}} \right)
\end{align*}
\]

(30)

If the extracted values of \(\text{Proof}^\gamma_{\text{Final}}^{\text{RSU}}, \text{Proof}^\gamma_{\text{Final}}^{\text{RSU}}\), and the hashed value \(H_4 \left( TS^2_{\text{CDA}}, ID^2_j, \text{Proof}^\gamma_{\text{Final}}^{\text{RSU}} \right)\) matches the information in its storage, vehicle confirms the validity of RSU₂.

Finally, the cross-domain authentication design with RSU₂ is finished. Identity of vehicle can be verified by the other RSUs without accessing the remote VC. Moreover, in order for successive cross-domain authentication \(V_j \leftrightarrow \text{RSU}_k \in \{\text{RSU}_3, \text{RSU}_4, \ldots, \text{RSU}_n\}\), RSU₂ will simultaneously broadcast the packet \(\langle ID^2_j, Q_j, \xi_j, \text{Proof}^\gamma_{\text{Final}}^{\text{CDA}}, \text{Cert}_{\text{Final}}^{\text{CDA}} \rangle\) to all its neighboring RSUs through wired edge networks. Upon receiving the packet, all its neighboring RSUs temporarily store it in their storage for possible further use. If not required in certain time interval \(\Delta_{\text{CDA}}\), the packet is abandoned. Please note that

\[
\text{Cert}_{\text{Final}}^{\text{CDA}} = h_3 \left( ID^2_j, Q_j, \xi_j, \text{Proof}^\gamma_{\text{Final}}^{\text{CDA}} \right).
\]

Following this way, in the next \(k\) cross-domain authenticating sessions, \(\langle ID^2_j, Q_j, \xi_j, \text{Proof}^\gamma_{\text{Final}}^{\text{CDA}}, \text{Cert}_{\text{Final}}^{\text{CDA}} \rangle\) will be broadcast by RSUₖ, where

\[
\begin{align*}
\text{ID}^k_j &= h_2 \left( \text{ID}^{k-1}_j, r^\text{CDA}_j \right) \\
\text{Proof}^\gamma_{\text{Final}}^{\text{CDA}}_{[j,k]} &= \text{Proof}^\gamma_{\text{Final}}^{\text{CDA}}_{[j,k-1]} | \text{Proof}^\gamma_{\text{Final}}^{\text{RSU}}_{[j,k-1]} | \text{Enc}_{\langle Q_i, \xi_i\rangle}^{\text{RSU}} \left( h_2 \left( \text{ID}^k_j, r^\text{CDA}_j, r^\text{RSU}_j \right) \right)
\end{align*}
\]

(31)

Please note that \(r^\text{CDA}_j \in \mathbb{Z}_q^*\) and \(r^\text{RSU}_j \in \mathbb{Z}_q^*\) refers to the generated random numbers that are only effective within each successful authentication session. Intuitively, the anonymous identity for individual vehicle is updated in each session as \(\text{ID}^k_j = h_2 \left( \text{ID}^{k-1}_j, r^\text{CDA}_j \right)\). The \(\text{Proof}^\gamma_{\text{Final}}^{\text{CDA}}_{[j,k]}\) is calculated according to the previous two valid proofs and the characteristics of the current RSUₖ. Our cross-domain authentication mechanism can be performed in this way.

5. Security Analysis

In this section, the corresponding proofs on featured security properties of the proposed HCDA scheme are given. The comparisons in terms of the major security characteristics with the state-of-the-art are presented.
5.1. Security Proofs

**Theorem 1.** The cross-domain verification process is proven to be correct if and only if the credential is successfully issued following the device registration, mutual authentication, and cross-domain authentication strategy.

**Proof of Theorem 1.** As mentioned above, for individual vehicle with previously allocated identity $ID_j$, its vehicle partial secret key pair and the homographic encryption key pair is extracted as $(k_j, r_j)$ and $(Q_j, \xi_j)$, respectively. With the vehicle path RSU$_{k-1}$ → RSU$_k$ $(k \in [1, n])$, vehicle is approaching the effective domain of RSU$_k$ on timepoint $t_k$, while the RSU parameters set $\langle T_{RSU}^k, ID^k_{RSU}, O_k, h_k, R^k, Cert^k_{RSU} \rangle$ is periodically broadcast by RSU$_k$ (index $i \leftarrow k$). That is

$$\begin{align*}
\begin{cases}
\mathcal{R}^k = \mathcal{R}^k_{RSU} P \\
Cert^k_{RSU} = H_1 \left( T_{RSU}^k, ID^k_{RSU}, O_k, h_k, R^k \right)
\end{cases}
\end{align*}
$$

(32)

where partial secret key pair and the homographic encryption key pair for RSU$_k$ is extracted as $\langle k^k_{RSU}, R^k_{RSU} \rangle$ and $(O_k, h_k)$, respectively.

Following this way, in the $k$-cross domain authenticating sessions, RSU$_k$ has already acquired $\langle ID_{k-1}^k, Q_j, \xi_j, Proof_{CDA}^\sigma_{j, [k-1]} \rangle$ from the previous RSU$_{k-1}$ within certain time interval $\Delta_{CDA}$, where

$$\begin{align*}
\begin{cases}
ID_{k-1}^k = h_2 \left( ID_{k-2}^k, r_{CDA}^k \right) \\
Proof_{CDA}^\sigma_{j, [k-1]} = Proof_{CDA}^\sigma_{j, [k-2]} \cdot Proof_{CDA}^\sigma_{j, [k-1]} \\
Cert_{CDA}^\sigma_{j, [k-1]} = h_3 \left( ID_{k-1}^k, Q_j, \xi_j, Proof_{CDA}^\sigma_{j, [k-1]} \right)
\end{cases}
\end{align*}
$$

(33)

Meanwhile, vehicle generates the new random number $r_{CDA}^k \in \mathbb{Z}_q^*$ and calculates the corresponding proof and credential as

$$\begin{align*}
\begin{cases}
Proof_{CDA}^\sigma_{j, [k-1]} = Enc_{j, [k-1]}^C \left( 2^{k-2} \omega_j - h_2 \left( ID_{k-1}^k, r_{CDA}^k \right) \right) \\
Credential_{[k-1]} = h_4 \left( Enc_{j, [k-1]}^C \left( 2^{k-2} \omega_j \right) \right)
\end{cases}
\end{align*}
$$

(34)

In this case, RSU$_k$ extracts $Proof_{CDA}^\sigma_{j, [k-1]}$ from the stored packet, and $\langle Proof_{CDA}^\sigma_{j, [k-1]}, Credential_{j, [k-1]} \rangle$ from the fast authentication packet. The validation on $h_4 \left( Proof_{CDA}^\sigma_{j, [k-1]}, Proof_{CDA}^\sigma_{j, [k-1]} \right) = Credential_{j, [k-1]}$ is performed. The correctness can be elaborated as

L.H.S.

$$\begin{align*}
&= h_4 \left( Proof_{CDA}^\sigma_{j, [k-1]} \right) \\
&= h_4 \left( Proof_{CDA}^\sigma_{j, [k-2]} \cdot Proof_{CDA}^\sigma_{j, [k-1]} \right) \\
&= h_4 \left( Proof_{CDA}^\sigma_{j, [k-2]} \cdot Proof_{CDA}^\sigma_{j, [k-1]} \cdot Enc_{j, [k-1]}^{C_{RSU}} \left( 2^{k-2} \omega_j \right) \cdot Enc_{j, [k-1]}^{CDA} \left( 2^{k-2} \omega_j \right) \right) \\
&= h_4 \left( Proof_{CDA}^\sigma_{j, [k-2]} \cdot Proof_{CDA}^\sigma_{j, [k-1]} \cdot Enc_{j, [k-1]}^{C_{RSU}} \left( 2^{k-2} \omega_j \right) \cdot Enc_{j, [k-1]}^{CDA} \left( 2^{k-2} \omega_j \right) \right) \\
&= h_4 \left( Proof_{CDA}^\sigma_{j, [k-2]} \cdot Proof_{CDA}^\sigma_{j, [k-1]} \cdot Enc_{j, [k-1]}^{C_{RSU}} \left( 2^{k-2} \omega_j \right) \cdot Enc_{j, [k-1]}^{CDA} \left( 2^{k-2} \omega_j \right) \right)
\end{align*}
$$

(35)
Since vehicle has successfully passed the verification process within the previous \((k-1)\) domains, we can extract

\[
\begin{align*}
    h_4 \left( \text{Proof}_{[1]}^\sim \cdot \text{Proof}_{[1]}^- \right) & = \text{Credential}_{[1]} \rightarrow h_4 \left( \text{Enc}_{(Q, \tilde{\phi})}^{\text{CDA}} \left[ 2\omega_j \right] \right) \\
    h_4 \left( \text{Proof}_{[2]}^\sim \cdot \text{Proof}_{[2]}^- \right) & = \text{Credential}_{[2]} \rightarrow h_4 \left( \text{Enc}_{(Q, \tilde{\phi})}^{\text{CDA}} \left[ 2^2\omega_j \right] \right) \\
    \vdots \ & \vdots \\
    h_4 \left( \text{Proof}_{[k-2]}^\sim \cdot \text{Proof}_{[k-2]}^- \right) & = \text{Credential}_{[k-2]} \rightarrow h_4 \left( \text{Enc}_{(Q, \tilde{\phi})}^{\text{CDA}} \left[ 2^{k-2}\omega_j \right] \right)
\end{align*}
\]

Hence, \( h_4 \left( \text{Proof}_{[k-2]}^\sim \cdot \text{Proof}_{[k-2]}^- \right) = \text{Enc}_{(Q, \tilde{\phi})}^{\text{CDA}} \left[ 2^{k-2}\omega_j \right] \) holds. In this case,

\[
\begin{align*}
    L.H.S. \\
    = h_4 \left( \text{Proof}_{[k-2]}^\sim \cdot \text{Proof}_{[k-2]}^- \cdot \text{Enc}_{(Q, \tilde{\phi})}^{\text{CDA}} \left[ 2^{k-2}\omega_j \right] \right) \\
    = h_4 \left( \text{Enc}_{(Q, \tilde{\phi})}^{\text{CDA}} \left[ 2^{k-2}\omega_j \right] \cdot \text{Enc}_{(Q, \tilde{\phi})}^{\text{CDA}} \left[ 2^{k-2}\omega_j \right] \right) \\
    = h_4 \left( \text{Enc}_{(Q, \tilde{\phi})}^{\text{CDA}} \left[ 2^{k-1}\omega_j \right] \right)
\end{align*}
\]

Meanwhile,

\[
\begin{align*}
    \text{Credential}_{[k-1]} \\
    = h_4 \left( \text{Enc}_{(Q, \tilde{\phi})}^{\text{CDA}} \left[ 2^{k-1}\omega_j \right] \right). \\
    = L.H.S.
\end{align*}
\]

Hence, \( L.H.S. = R.H.S. \) holds. The correctness of \( h_4 \left( \text{Proof}_{[k-2]}^\sim \cdot \text{Proof}_{[k-2]}^- \right) \) can be proved. In conclusion, the proposed cross-domain authentication mechanism is proved to be correct if the certificate is successfully issued.

**Theorem 2.** Dynamic key updating is conducted during each successful validation session. Message unlinkability among all participating semi-trustworthy RSUs can be provided.

**Proof of Theorem 2.** Assuming certain vehicle follows path \( \text{RSU}_1 \rightarrow \text{RSU}_n \) and has passed through \( k \) cross-domain authenticating sessions, \( \text{RSU}_k \) \((k \in [1,n])\) acquires \( \left\{ ID_{k-1}^k, Q, \tilde{\phi}, \text{Proof}_{[k-1]}^\sim, \text{Cert}_{[k-1]}^{\text{CDA}} \right\} \) from its previous \( \text{RSU}_{k-1} \). After successful mutual authentication with \( \text{RSU}_k \), \( \left\{ ID_k^k, Q, \tilde{\phi}, \text{Proof}_{[k]}^\sim, \text{Cert}_{[k]}^{\text{CDA}} \right\} \) will be broadcast from \( \text{RSU}_k \) to \( \text{RSU}_{k+1} \). Please note that the anonymous vehicle identity is dynamically updated as \( ID_k^k = h_2 \left( ID_{k-1}^k, r_j^{\text{CDA}} \right) \), along with the corresponding proof updated as \( \text{Proof}_{[k]}^\sim = \text{Proof}_{[k-1]}^\sim \cdot \text{Enc}_{(Q, \tilde{\phi})}^{\text{CDA}} \left[ h_2 \left( ID_{RSU}^{k}, r_j^{\text{CDA}} \right) \right] \). In this way, vehicle anonymity can be guaranteed during all \( n \) cross-domain authenticating sessions. Particularly, with random number \( r_j^{\text{CDA}} \in Z_q^* \) generated by current RSU, the one-way mapping between \( ID_{k-1}^k \rightarrow ID_k^k \) is known only to \( \text{RSU}_k \) of current domain, while the successive \( \text{RSU}_{k+1} \) cannot trace the anonymous identity from the acquired \( ID_k^k \). That is, each RSU has zero knowledge about the vehicle identity out of its domains, which significantly reduces the risk of message linkability across various domains. In this case, the semi-trustworthy RSUs cannot acquire confidential information about certain vehicles. Illegal tracing towards vehicle can be prevented as well. Even in worse situations with compromised RSUs, the adopted session key \( sk_j = H_5 \left( k, r_j, P \right) \) is shared among \( \text{VC} \) and vehicle, while
kept secret to each RSU. Hence, impersonate attack by compromised RSUs is not possible in our design. In conclusion, message unlinkability and secure data transmission with semi-trustworthy RSUs can be provided. □

**Theorem 3.** Conditional identity privacy preserving is guaranteed. The dynamic anonymous identities used during all authentication sessions offer untraceability towards specific vehicle, while the remote VC is able to trace the real identity of malicious devices if necessary.

**Proof of Theorem 3.** In device registration, the unique records regarding all registered vehicles and RSUs are safely stored in vehicular cloud. The key pair for vehicle is defined as $\langle ID_V^l, k_l \rangle$. Similarly, the confidential RSU information set $\langle ID_{RSU}^l, s_{RSU}^l \rangle$ is safely shared among VC and each RSU. Please note that the distinctive identity $ID_V^l$ and $ID_{RSU}^l$ remain hidden all the time. For individual RSU, the adopted anonymous identity $ID_{RSU}^l$ is issued as $ID_{RSU}^l = h_1(TS_1^l, ID_V^l, r_{RSU}^l, s_{RSU}^l, P)$, where the fresh timestamp $TS_1^l$ and the randomly generated $r_{RSU}^l \in \mathbb{Z}_q$ provide uncertainty in generation of $ID_{RSU}^l$. With obvious time feature, each $ID_{RSU}^l$ is only valid within certain time period and will expire in future. As for each vehicle, anonymous identity used in the initial authentication session is computed as $ID_1^l = h_2(\langle ID_V^l, r_P^l \rangle)$, while after the initial validation, RSU update the vehicle identity as $ID_1^l = h_2(\langle ID_V^l, r_{RSU}^l, s_{RSU}^l, P \rangle)$, where the RSU key pair $\langle r_{RSU}^l, s_{RSU}^l \rangle$ is adopted. Subsequently, the dynamic updating for anonymous identity is computed as $ID_1^l = h_2(\langle ID_V^l, r_{RSU}^l, s_{RSU}^l, P \rangle)$, which is the hashed value of previous identity and current random number $r_{RSU}^l \in \mathbb{Z}_q$. In this way, anonymous identities for both RSUs and vehicles are provided. The malicious devices cannot illegally trace certain vehicle through eavesdropping the transmitted messages. On the other hand, by retrieving the entire vehicle path $RSU_1 \rightarrow RSU_n$, VC is able to reveal the original identity, which is crucial for detecting and revoking the compromised VANET entities. Conditional identity privacy preserving is enabled in this way. □

**Theorem 4.** The proposed design is resistant to replay attack during the whole authentication process. The historical messages from past sessions cannot pass the current validation.

**Proof of Theorem 4.** In device registration, mutual authentication, and cross-domain authentication phases, the fresh timestamps set $\{TS_1^l, TS_2^l, TS_3^l, TS_4^l, TS_{CDA}^l\}$ are used in each communication round. Meanwhile, the certificates involving all transmitted elements are presented. For example, in mutual authentication phase, vehicle sends the requesting packet $\langle \text{Request}, TS_3^l, ID_V, Y, Cert_V^l \rangle$ to RSU for verification, where the certificate $Cert_V^l = \text{Enc}_{(\mathbb{O}, A)}^{\Gamma} [\{N_j, Q_j, \xi_j \mid |\mathcal{J}_i\}]$ is conducted based on the intermediate values $\langle N_j, \mathcal{J}_i \rangle$. Please note that both $N_j$ and $\mathcal{J}_i$ are relate to timestamp $TS_3^l$. In this case, assuming that in specific timepoint $T_A$, adversary $\mathcal{A}_1$ has access to all the $z$ transmitted requesting packets during time interval $[T_H, T_C]$, where $T_C < T_A$. In this case, the acquired $z$ packets can be presented as $\langle \text{Request}, TS_3^l, ID_V, Y, Cert_V^l \rangle_{I \in [1, z]}$, where vehicle $\{V_1, \ldots, V_z\}$ are involved. Intuitively, the direct message replaying with historical packets cannot pass the RSU validation since $TS_3^l < T_C < T_A$ for all $I \in [1, z]$. Hence, $\mathcal{A}_1$ acquires current timestamp $T_A$ of $T_A$ and manages to generate the modified certificate $Cert_V^l$. Intuitively, the probability for $Cert_V^l$ to pass the verification is $\frac{1}{2^y}$, where the length of output $Cert_V^l$ is assumed to be $y$. Hence, our design is resistant to replay attack. □

**Theorem 5.** A certificateless authentication infrastructure is adopted for all VANET entities in the proposed design. The intrinsic key escrow problem of identity-based cryptography can be addressed. No-repudiation for specific vehicle is provided accordingly.
**Proof of Theorem 5.** As mentioned above, during the device registration phase, the distinctive identity for a vehicle is allocated as \( ID_j^V \), while the assigned secret key is \( k_j \). Please note that \( k_j \) is stored in VC record and shared between VC and vehicle. Subsequently, vehicle itself randomly generates its own partial secret key \( r_j \in \mathbb{Z}_q^* \), which will be kept secret to VC. In this way, the partial secret key pair is set as \( \langle k_j, r_j \rangle \), while VC has no access to \( r_j \). Afterwards, with the characteristics of elliptic curve discrete logarithm problem, other VANET entities cannot extract \( r_j \) from the published \( ID_j = h_2 \left( ID_j^V, r_j P \right) \) or \( Y_j = r_j R_i \), given the value of \( R_i \). Similarly, the partial secret key is defined as \( \langle r_i^{RSU}, s_i^{RSU} \rangle \), where \( r_i^{RSU} \in \mathbb{Z}_q^* \) is randomly generated by RSU during registration and kept confidential to all other entities including VC. In other words, VC does not have full control over the participating vehicles and RSUs. □

**Theorem 6.** In the proposed scheme, VC and RSUs cannot frame an innocent vehicle or accuse the honest vehicle of misbehaviors.

**Proof of Theorem 6.** Initially, the essential vehicle partial secret key is generated as \( \langle k_j, r_j \rangle \), where VC has no access to \( r_j \). Upon validation, the session key established between VC and vehicle is issued as \( sk_j = H_5 \left( k_j r_j P \right) \), which is used as the unique identifying code shared between vehicle and VC. Please note that VC cannot issue or modified the shared \( sk_j \) due to ignorance on the \( r_j \) generated my vehicle itself. In this case, VC cannot authenticate itself to vehicle and pass the final authentication process on \( \omega_j = h_2 \left( ID_j^V, k_j r_j P \right) \). In subsequent data transmission, the adopted homographic encryption mechanism is able to guarantee the message security. As for RSUs, the time-related vehicle anonymous identity and valid key information cannot be forged or decrypted. Overall, the non-frameability for a specific vehicle can be guaranteed. □

5.2. **Security Properties Comparison**

The proposed protocol is compared with the state-of-the-art VANET authentication and key agreement schemes including ICPP [37], SAKM [43], and PFCA [44]. The comparison results are presented in Table 3, proving that the proposed scheme satisfies the desired security requirements.

| Scheme                        | ICPP [37] | SAKM [43] | PFCA [44] | The Proposed Scheme |
|-------------------------------|-----------|-----------|-----------|---------------------|
| Cross-Domain Authentication   | ×         | ×         | ×         | √                   |
| Unforgeability                | √         | √         | √         | √                   |
| Replay Attack Resistance      | √         | √         | √         | √                   |
| Conditional Privacy Preserving| √         | √         | √         | √                   |
| Session Key Establishment     | √         | √         | √         | √                   |
| Key Escrow Resilience         | √         | √         | √         | √                   |
| Scalability                   | ×         | √         | √         | √                   |
| Anonymous Identity Updating   | ×         | ×         | ×         | √                   |
| Modification Attack Resistance| √         | √         | √         | √                   |
| Collusion Attack Resilience   | √         | ×         | √         | √                   |
| Sybil Attack Resilience       | √         | ×         | √         | √                   |

6. **Performance Analysis**

Performance analysis of the proposed scheme is presented in this section, which specifically emphasizes on the crucial properties for resource-limited VANET environment: storage overhead, computation cost, and communication cost.
6.1. Storage Overhead

In practical VANETs environment, both vehicles and the RSUs perform as the basic units in VANETs communication. The state-of-the-art VANETs authentication schemes including ICPP [37], SAKM [43], and PFCA [44] are analyzed. Hence, advantages of our scheme can be shown as shown in the comparison.

In device registration, the distinctive identity \( ID_i \) and correlated partial secret key pair \( \langle r_i, s_i \rangle \) for individual RSU are safely stored. Upon registration, the current RSU anonymous identity \( ID_i^{RSU} \) is generated. Subsequently, the key generation for homomorphic encryption infrastructure is conducted. Both encryption key pair \( \langle O_i, h_i \rangle \) and decryption key pair \( \langle A_i, \bar{h}_i \rangle \) are issued. Relevant calculations on the RSU parameters set \( \langle TS_i^1, ID_i^{RSU}, O_i, h_i, \bar{h}_i, R_i, Cert_i^{RSU} \rangle \) is periodically executed. Accordingly, we define the length of the identity and secret key such as \( ID_i \) and \( s_i \) respectively denoted as \( p \) and \( q \).

In VANETs communication, the state-of-the-art VANETs authentication schemes including ICPP [37], SAKM [43], and PFCA [44] are analyzed. Hence, advantages of our scheme can be shown as shown in the comparison.

In vehicle side, the original vehicle identity \( ID_j \) and the related partial secret key \( k_j \) is stored. In mutual authentication, the randomly generated \( r_j \in Z_n^* \), as well as the anonymous identity is generated. Moreover, the vehicle homomorphic encryption key pair \( \langle Q_j, \xi_j \rangle \) and the decryption key pair \( \langle \Gamma_j, \psi_j \rangle \) are distributed. With the published RSU parameter set \( \langle TS_j^2, ID_j^{RSU}, O_j, h_j, \bar{h}_j, R_j, Cert_j^{RSU} \rangle \), vehicle delivered the requesting packet \( \langle \text{Request}, TS_j^3, ID_j, Y_j, Cert_j^{RV} \rangle \) to RSU. The packet \( \langle TS_j^4, ID_j, Cert_j^{RSU}, \Phi_j \rangle \) is generated finally. Please note that the delivered session key \( s_k \) is stored as well. Hence, the total computation cost for individual vehicle is \( 32 \times 13 + 256 \times 3 + 160 \times 2 + 24 \times 3 = 1576 \) bits. Comparison results with existing VANETs authentication schemes are shown in Table 4.

6.2. Computation Cost

The computation cost of the proposed authentication scheme is presented in this section. For better description, The employed secure hash functions, multiplication, and exponential operation are respectively denoted as \( H, M \) and \( E \). The point multiplication and the pairing operation are respectively denoted as \( \text{p} \) and \( \text{e} \). The comparison results on computation cost is shown in Table 5, where the approximate execution time is given according to [43]. Complex pairing computations are not adopted. Hence, less computation overhead for resource limited vehicles is required, which is of significance to practical VANET scenarios.

| Scheme | ICPP [37] | SAKM [43] | PFCA [44] | The Proposed Scheme |
|--------|-----------|-----------|-----------|---------------------|
| Storage Cost (RSU) | 1760n + 1056 bits | 1616n + 1360 bits | 3992n + 1376 bits | 880n + 1008 bits |
| Storage Cost (Vehicle) | 2112 bits | 2208 bits | 4368 bits | 1576 bits |
Table 5. Comparison Result of Computation Cost.

| Scheme          | ICPP [37]          | SAKM [43]          | PFCA [44]          | The Proposed Scheme |
|-----------------|--------------------|--------------------|--------------------|--------------------|
| Computation Cost (RSU) | \((2n + 2)p + 3nM \approx (3.418n + 3.418)\) ms | \((2n + 2)p + (2n + 3)H + 2nEx + (n + 1)H \approx (1.76n + 10.184)\) ms | \((5n + 3)p + (2n + 3)H + 2nEx + (n + 1)p + (2n + 2)H + (4n + 2)Ex + 8 \approx (8.545n + 5.127)\) ms | \((n + 1)p + (2n + 2)H + (4n + 2)Ex + 8 \approx (1.143n + 8.973)\) ms |
| Vehicle         | \((3p + 3H + 2nM \approx (2.041)\) ms | \((3p + 3H + 8 \approx (1.869)\) ms | \((4p + 5H + 6Ex \approx (3.632)\) ms | \((p + 4H + 4Ex \approx (1.477)\) ms |

6.3. Communication Cost

The communication rounds for the VANETs’ authentication in RSU side is discussed in this section, where a total of \(n\) vehicles are to be successfully verified. Furthermore, the same path \(RSU_1 \rightarrow RSU_k\) is assumed, where \(k\) cross-domain authentication sessions are conducted. In this case, the initial communication rounds with single vehicles is \(2n\) in total. Accordingly, the communication cost is given in Table 6, proving that less communication rounds are required compared to the state-of-the-art.

Table 6. Comparison Results of Communication Cost.

| Scheme                          | ICPP [37]          | SAKM [43]          | PFCA [44]          | The Proposed Scheme |
|---------------------------------|--------------------|--------------------|--------------------|--------------------|
| Communication Rounds (Initial Validation) | \(4n + 2\) | \(2n + 1\) | \(2n\) | \(2n\) |
| Communication Rounds (Cross-Domain Validation) | \(\slash\) | \(\slash\) | \(\slash\) | \(2n\) |

7. Conclusions

In this paper, the cross-domain authentication issue is further studied under the cloud-assisted VANET infrastructure with edge RSU clusters. In our design, the successive RSUs could efficiently verify the cross-domain vehicle with the transited certificate from the neighbor RSUs and vehicle itself, while the identity and secrets of each vehicle is hidden all the time. In this case, the semi-trusted RSUs cannot access the confidential information from the remote cloud server, thus the balance between efficiency and security is properly made. Meanwhile, homographic encryption cryptography is adopted. Dynamic updating towards the anonymous vehicle identity is conducted upon each successful validation, where conditional privacy preserving is enabled in this way. Advanced security properties is guaranteed in our design, while performance discussion demonstrates its efficiency.

Author Contributions: Conceptualization, H.T. and I.C.; Methodology, H.T.; Formal analysis, H.T.; Investigation, S.X.; Writing—Original Draft Preparation, H.T.; Writing—Review and Editing, H.T. and S.X.; Supervision, I.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by Chosun University (2020).

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

References
1. Li, Y.; Chen, W.; Cai, Z.; Fang, Y. CAKA: A Novel Certificateless-Based Cross-Domain Authenticated Key Agreement Protocol for Wireless Mesh Networks. Wirel. Netw. 2016, 22, 2523–2535. [CrossRef]
2. Feng, Q.; He, D.; Zeadally, S.; Liang, K. BPAS: Blockchain-Assisted Privacy-Preserving Authentication System for Vehicular Ad Hoc Networks. IEEE Trans. Ind. Inform. 2020, 16, 4146–4155. [CrossRef]
3. Tan, H.; Guı, Z.; Chung, I. A Secure and Efficient Certificateless Authentication Scheme With Unsupervised Anomaly Detection in VANETs. IEEE Access 2018, 6, 74260–74276. [CrossRef]
4. Yao, Y.; Chang, X.; Mišić, J.; Mišić, V.B.; Li, L. BLA: Blockchain-Assisted Lightweight Anonymous Authentication for Distributed Vehicular Fog Services. IEEE Internet Things J. 2019, 6, 5775–5784. [CrossRef]
5. He, D.; Kumar, N.; Wang, H.; Wang, L.; Choo, K.R.; Vinel, A. A Provably-Secure Cross-Domain Handshake Scheme with Symptoms-Matching for Mobile Healthcare Social Network. IEEE Trans. Dependable Secur. Comput. 2018, 15, 633–645. [CrossRef]
6. Cui, J.; Wei, L.; Zhang, J.; Xu, Y.; Zhong, H. An Efficient Message-Authentication Scheme Based on Edge Computing for Vehicular Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* 2019, 20, 1621–1632. [CrossRef]

7. Shen, J.; Tan, H.; Ren, Y.; Liu, Q.; Wang, B. A Practical RFID Grouping Authentication Protocol in Multiple-Tag Arrangement With Adequate Security Assurance. In Proceedings of the 2016 18th International Conference on Advanced Communication Technology (ICACT), Dublin, Ireland, 31 January–3 February 2016; pp. 693–699.

8. Lu, Z.; Wang, Q.; Gu, G.; Zhang, H.; Liu, Z. A Blockchain-Based Privacy-Preserving Authentication Scheme for VANETs. *IEEE Trans. Very Large Scale Integr. VLSI Syst.* 2019, 27, 2792–2801. [CrossRef]

9. Liu, B.; Jia, D.; Wang, J.; Lu, K.; Wu, L. Cloud-Assisted Safety Message Dissemination in VANET–Cellular Heterogeneous Wireless Network. *IEEE Syst. J.* 2017, 11, 128–139. [CrossRef]

10. Kayes, A.; Rahayu, W.; Watters, P.; Alazab, M.; Dillon, T.; Chang, E. Achieving Security Scalability and Flexibility Using Fog-Based Context-Aware Access Control. *Future Gener. Comput. Syst.* 2020, 107, 307–323. [CrossRef]

11. Yu, S.; Park, K.; Park, Y. A Secure Lightweight Three-Factor Authentication Scheme for IoT in Cloud Computing Environment. *Future Gener. Comput. Syst.* 2019, 19, 3598. [CrossRef]

12. Lee, J.; Yu, S.; Park, K.; Park, Y. Secure Three-Factor Authentication Protocol for Multi-Gateway IoT Environments. *Sensors* 2019, 22, 2358. [CrossRef] [PubMed]

13. Wang, F.; Xu, Y.; Zhang, H.; Zhang, Y.; Zhu, L. 2FLIP: A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANET. *IEEE Trans. Veh. Technol.* 2016, 65, 896–911. [CrossRef]

14. Tan, H.; Choi, D.; Kim, P.; Pan, S.; Chung, I. Comments on ‘Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks’. *IEEE Trans. Intell. Transp. Syst.* 2017, 19, 2149–2151. [CrossRef]

15. Du, X.; Xiao, Y.; Ci, S.; Guizani, M.; Chen, H. A Routing-Driven Key Management Scheme for Heterogeneous Sensor Networks. In Proceedings of the 2007 IEEE International Conference on Communications, Glasgow, Scotland, 24–28 June 2007; pp. 3407–3412.

16. Ullah, A.; Yaqoob, S.; Imran, M.; Ning, H. Emergency Message Dissemination Schemes Based on Congestion Avoidance in VANET and Vehicular Fog Computing. *IEEE Access* 2019, 7, 1570–1585. [CrossRef]

17. Tan, H.; Chung, I. Secure Authentication and Group Key Distribution Scheme for WBANs Based on Smartphone ECG Sensor. *IEEE Access* 2019, 7, 151459–151474. [CrossRef]

18. Zhu, X.; Jiang, S.; Wang, L.; Li, H. Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks. *IEEE Trans. Veh. Technol.* 2014, 63, 907–919. [CrossRef]

19. Zhou, T.; Shen, J.; Li, X.; Wang, C.; Tan, H. Logarithmic Encryption Scheme for Cyber-Physical Systems Employing Fibonacci Q-matrix. *Future Gener. Comput. Syst.* 2020, 108, 1307–1313. [CrossRef]

20. Huang, D.; Misra, S.; Verma, M.; Xue, G. PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs. *IEEE Trans. Intell. Transp. Syst.* 2011, 12, 736–746. [CrossRef]

21. Tian, Z.; Shi, W.; Wang, Y.; Zhu, C.; Du, X.; Su, S.; Sun, Y.; Guizani, N. Real-Time Lateral Movement Detection Based on Evidence Reasoning Network for Edge Computing Environment. *IEEE Trans. Ind. Inform.* 2019, 15, 4285–4294. [CrossRef]

22. Shen, J.; Tan, H.; Zhang, Y.; Sun, X.; Xiang, Y. A New Lightweight RFID Grouping Authentication Protocol for Multiple Tags in Mobile Environment. *Multimed. Tools Appl.* 2017, 76, 22761–22783. [CrossRef]

23. Ma, M.; He, D.; Wang, H.; Kumar, N.; Choo, K.R. An Efficient and Provably Secure Authenticated Key Agreement Protocol for Fog-Based Vehicular Ad-Hoc Networks. *IEEE Internet Things J.* 2019, 6, 8065–8075. [CrossRef]

24. Tan, H.; Chung, I. A Secure and Efficient Group Key Management Protocol with Cooperative Sensor Association in WBANs. *Sensors* 2018, 18, 3930. [CrossRef] [PubMed]

25. Wasef, A.; Shen, X. EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks. *IEEE Trans. Mob. Comput.* 2013, 12, 78–89. [CrossRef]

26. Kaur, K.; Garg, S.; Kaddoum, G.; Gagnon, F.; Ahmed, S.H. Blockchain-Based Lightweight Authentication Mechanism for Vehicular Fog Infrastructure. In Proceedings of the 2019 IEEE International Conference on Communications Workshops (ICC Workshops), Shanghai, China, 20–24 May 2019; pp. 1–6.

27. Chuang, M.; Lee, J. TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks. *IEEE Syst. J.* 2014, 8, 749–758. [CrossRef]
28. Tan, H.; Song, Y.; Xuan, S.; Pan, S.; Chung, I. Secure D2D Group Authentication Employing Smartphone Sensor Behavior Analysis. *Symmetry* **2018**, **11**, 969. [CrossRef]
29. Li, J.; Lu, H.; Guizani, M. ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs. *IEEE Trans. Parallel Distrib. Syst.* **2015**, **26**, 938–948. [CrossRef]
30. Alazzawi, M.A.; Lu, H.; Yassin, A.A.; Chen, K. Efficient Conditional Anonymity With Message Integrity and Authentication in a Vehicular Ad-Hoc Network. *IEEE Access* **2019**, **7**, 71424–71435. [CrossRef]
31. Tan, H.; Choi, D.; Kim, P.; Pan, S.; Chung, I. An Efficient Hash-based RFID Grouping Authentication Protocol Providing Missing Tags Detection. *J. Internet Technol.* **2018**, **19**, 481–488.
32. Hao, Y.; Cheng, Y.; Zhou, C.; Song, W. A Distributed Key Management Framework with Cooperative Message Authentication in VANETs. *IEEE J. Sel. Areas Commun.* **2011**, **29**, 616–629. [CrossRef]
33. Wang, B.; Wang, Y.; Chen, R. A Practical Authentication Framework for VANETs. *Secur. Commun. Netw.* **2019**, 1–11. [CrossRef]
34. Tan, H.; Choi, D.; Kim, P.; Pan, S.; Chung, I. Secure Certificateless Authentication and Road Message Dissemination Protocol in VANETs. *Wirel. Commun. Mob. Comput.* **2018**, 2018, 1–13. [CrossRef]
35. Zhang, L.; Wu, Q.; Solanas, A.; Domingo-Ferrer, J. A Scalable Robust Authentication Protocol for Secure Vehicular Communications. *IEEE Trans. Veh. Technol.* **2010**, **59**, 1606–1617. [CrossRef]
36. Lu, R.; Lin, X.; Liang, X.; Shen, X. A Dynamic Privacy-Preserving Key Management Scheme for Location-Based Services in VANETs. *IEEE Trans. Intel. Transp. Syst.* **2012**, **13**, 127–139. [CrossRef]
37. He, D.; Zeadally, S.; Xu, B.; Huang, X. An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks. *IEEE Trans. Inf. Forensics Secur.* **2015**, **10**, 2681–2691. [CrossRef]
38. Lo, N.; Tsai, J. An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks Without Pairings. *IEEE Trans. Intel. Transp. Syst.* **2016**, **17**, 1319–1328. [CrossRef]
39. Shao, J.; Lin, X.; Lu, R.; Zuo, C. A Threshold Anonymous Authentication Protocol for VANETs. *IEEE Trans. Veh. Technol.* **2016**, **65**, 1711–1720. [CrossRef]
40. Lin, C.; Deng, D.; Yao, C. Resource Allocation in Vehicular Cloud Computing Systems With Heterogeneous Vehicles and Roadside Units. *IEEE Internet Things J.* **2018**, **5**, 3692–3700. [CrossRef]
41. Wang, Y.; Ding, Y.; Wu, Q.; Wei, Y.; Qin, B.; Wang, H. Privacy-Preserving Cloud-Based Road Condition Monitoring With Source Authentication in VANETs. *IEEE Trans. Inf. Forensics Secur.* **2019**, **14**, 1779–1790. [CrossRef]
42. Zhang, Q.; Gan, Y.; Zhang, Q.; Wang, R.; Tan, Y. A Dynamic and Cross-Domain Authentication Asymmetric Group Key Agreement in Telemedicine Application. *IEEE Access* **2018**, **6**, 24064–24074.
43. Tan, H.; Chung, I. Secure Authentication and Key Management With Blockchain in VANETs. *IEEE Access* **2020**, **8**, 2482–2498. [CrossRef]
44. Gayathri, N.B.; Thumbur, G.; Reddy, P.V.; Muhammad, Z.U.R. Efficient Pairing-Free Certificateless Authentication Scheme With Batch Verification for Vehicular Ad-Hoc Networks. *IEEE Access* **2018**, **6**, 31808–31819. [CrossRef]

© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).