sensors

Article

Efficient Certificate-Less Aggregate Signature Scheme with Conditional Privacy-Preservation for Vehicular Ad Hoc Networks Enhanced Smart Grid System

Thokozani Felix Vallent [1,†], Damien Hanyurwimfura [1,†] and Chomora Mikeka [2,*]

[1] African Center of Exellence in Internet of Things (ACEIoT), College of Science and Technology, University of Rwanda, KN Street Nyarugenge, Kigali P.O. Box 3900, Rwanda; tfvallent@gmail.com (T.F.V.); dhanyurwimfura@ur.ac.rw (D.H.)

[2] Department of Physics, Chancellor College, University of Malawi, Zomba P.O. Box 280, Malawi

[*] Correspondence: cmikeka@cc.ac.mw; Tel.: +265-994-226-206

[†] These authors contributed equally to this research on their respective tasks.

Citation: Vallent, T.F.; Hanyurwimfura, D.; Mikeka, C. Efficient Certificate-Less Aggregate Signature Scheme with Conditional Privacy-Preservation for Vehicular Ad Hoc Networks Enhanced Smart Grid System. *Sensors* **2021**, *21*, 2900. https://doi.org/10.3390/s21092900

Academic Editor: Carlos Tavares Calafate

Received: 31 March 2021
Accepted: 9 April 2021
Published: 21 April 2021

Abstract: Vehicular Ad hoc networks (VANETs) as spontaneous wireless communication technology of vehicles has a wide range of applications like road safety, navigation and other electric car technologies, however its practicability is greatly hampered by cyber-attacks. Due to message broadcasting in an open environment during communication, VANETs are inherently vulnerable to security and privacy attacks. However to address the cyber-security issues with optimal computation overhead is a matter of current security research challenge. So this paper designs a secure and efficient certificate-less aggregate scheme (ECLAS) for VANETs applicable in a smart grid scenario. The proposed scheme is based on elliptic curve cryptography to provide conditional privacy-preservation by incorporating usage of time validated pseudo-identification for communicating vehicles besides sorting out the KGC (Key Generation Center) escrow problem. The proposed scheme is comparatively more efficient to relevant related research work because it precludes expensive computation operations likes bilinear pairings as shown by the performance evaluation. Similarly, communication cost is within the ideal range to most related works while considering the security requirements of VANETs system applicable in a smart grid environment.

Keywords: smart grid; vehicular ad hoc network; privacy-preserving; certificate-less; signature; aggregation

1. Introduction

Major advancement in wireless sensor networks (WSN), Internet of Things (IoT) and the advent of the big data paradigm has seen the birth of various network based advancements in cross-cutting technologies, such as VANETs, which support wireless communication within vehicles and road sign units (RSUs) for numerous applications like traffic safety, location based-services, electric vehicles (EVs) and electricity exchange services among others [1–6]. The smart grid is one such technology motivated by the development of WSN and IoT in its functionality. EV technology will result in the elevation of power consumption, unsustainable by means of a traditional electricity grid [7]. An obvious solution to sorting out EVs electricity demands is by formulating VANETs-enhanced smart grid, with a coordinated charging system that is responsive to efficient cost and electricity utilization by using communication technologies [8,9]. Thus, it is recommended that algorithms for security, authentication, information processing and data aggregation be of high-precision and efficiency to allow low communication latency for real-time pricing and optimal electricity dispatch decisions in a VANETs enhanced smart grid system [10,11]. The concept of VANETs is an advancement of mobile ad hoc networks (MANETs) where there is real-time communication between EVs and RSUs for electricity charging/discharging [7,12,13]. Typically, the topology of VANETs includes trusted authorities (TAs), RSUs and onboard Units (OBUs) mounted on vehicles [14–16]. The OBUs constantly cast the traffic related messages about vehicles facilitating various smart applications and technologies such as current vehicle location, time, speed, direction and traffic condition in every 100–300 ms [13,17,18]. As is the case with many communication network based technologies, VANETs is not an exception to face various cyber-security challenges in terms of data security and user privacy [19–22]. With secure and privacy protection addressed, the applications of VANETs in traffic management and control, traffic accident avoidance features, traffic vigilance, gas emission, EV charging and fuel consumption will be fully implementable [23]. So if the VANETs network system is not protected, adversaries may launch all sorts of attacks like data modification, impersonation, replay, denial of service attacks among others. For instance, there are attacks launched by rogue vehicles broadcasting fake instructions to cause traffic accidents and general confusion. Thus, in terms of message senders' legitimacy there should be security features when sending messages to check authentication and integrity [23,24]. To this effect many authentication schemes have been proposed using traditional public key cryptography (PKC) to secure a VANETs system [25,26]. In terms of privacy concerns, anonymity must be provided in the design of securing the message from an eavesdropping adversary. In this way the real identity of communicating party will not be known nor communication transactions be analyzed and linked to a particular VANETs participant. However, due to abuse of the anonymity feature, the pseudonym given to participating entities should be traceable and revocable, so that the TA can reveal the real identity of malicious vehicle under certain conditions [27]. Since OBUs have limited computation and storage capabilities, the use of less computation intensive cryptographic techniques is promoted so as to handle large message flow in the system and improve smooth communication. Certificate-less aggregate signature (CLAS) is one efficient technique that improves message authentication by utilizing batch calculation of which saves bandwidth. In CLAS n signatures on n distinct messages from n distinct users, are aggregated into a single short signature that can be verified at once as combined [28]. This approach is very helpful in VANETs where RSUs collects and aggregate a large number of signatures from individual participants signatures into one signature that is broadcasted to vehicles in the system to achieve a particular VANETs enhanced smart grid application, and this greatly enhances efficiency in verification and communication overhead [13,29]. Achieving efficiency by design is much encouraged to cope up with the computation capabilities of RSUs and OBUs by constructing the algorithms with lighter computation operations. To this effect, employing elliptic curve cryptography (ECC) based cryptosystems improves computation efficiency by a great margin and thereby a recommendable approach. Thus, we propose an efficient certificate-less aggregate scheme with conditional privacy-preservation by using the ECC approach. The proposed scheme satisfies security and privacy requirements for VANETs with optimal efficiency and rigorous security proof is provided. There are different modes of communications in VANETs such as vehicle-to-vehicle (V2V), vehicle-to-grid (V2G) and vehicle-to-infrastructure (V2I) and vehicle-to-everything (V2E), which use the short medium range communication protocol called dedicated short range communication (DSRC) to facilitate various vehicular network applications [30]. These computer sophisticated vehicles are being adopted for various smart services in intelligent transportation systems (ITS). The following security requirements are important for any WSN based system such as VANETs:

- Non-repudiation: Any electric vehicle transaction has economic value and this can motivate fraudulent acts by the entities selling or buying electricity. Therefore, this measure of non-repudiation ensures that any electricity transaction can be accounted for, to the involved parties and any modification cannot be denied by the party.
- Message integrity and authentication: In a similar manner, any network transaction once completed cannot be modified by any malicious entity and once there is an attempt to tamper with the transaction, then it should be detectable by any legal entity of the system.

- Privacy: The actual identity of a consumer nor the information of a transaction in the network should not be known by any malicious party eavesdropping on the communications involving a particular targeted entity.
- Unlinkability: By observing the transactions in the VANETs network the entity's activities should still not be analysed and be associated with a particular RSU or vehicle. Thus to say messages plying on the network for any participant should still look random to an attacker and nothing associated with the participant should be determined.
- Traceability: However, for the undesirable conduct of an entity in the network such acts should be traced and be accounted for, against the individual. On the other hand the vehicle should be hidden or inaccessible from other unauthorized entities.
- Resistance to Attacks: Due to communication over a public channel, V2G security scheme must withstand various general attacks such as an impersonation attack, replay attack, modification attack, man-in-the-middle-attack and stolen verifier table attack in VANETs.

Therefore, we propose a novel anonymous certificate-less aggregate signature scheme for VANETs with conditional privacy-preservation in a smart grid system, that addresses common weaknesses of most existing certificate-less aggregate signature schemes. The main contribution of the paper can be summarized as follows:

- The proposed scheme achieves user anonymity with conditional privacy, such that each domain stores a Certificate Revocation List (CRL) in all road sign units located in that particular domain.
- The proposed scheme achieves optimal efficiency for certificate-less aggregate signature while precluding complex cryptographic operations like bilinear pairings and map-to-point hash operations.
- The proposed scheme withstand escrow property powers of the KGC but use of partial private key and user generated full private key for signature signing.

The rest of the paper is organized according to the outline given as follows—Section 2 reviews most relevant related works of CLAS schemes for VANETs. Section 3 provides the mathematical building blocks for the proposed scheme. Section 4 gives the detailed steps of the proposed work. Section 5, presents an indepth analysis of the scheme in terms of security, privacy and performance assessment. Finally, in Section 6 we give concluding remarks about the proposed scheme.

2. Related Works and Limitations

In VANETs, the source authentication and message integrity of traffic-related information form a very important security requirement in the system. Satisfaction of these security requirements ensure the trust and proper functionality of all versatile technologies that comes with a VANETs system by simply securing moving vehicles, RSUs, Application Servers, and roadside sensors. To this effect many research works have been done to provide the needed security for such an advent technology of smart city [24].

The key management problem posed by the certificate based PKI cryptosystem paved the way to the pioneering work of a certificate-less public key signature (CL-PKS) scheme by Al-Riyami and Paterson [31]. This idea caught much research interest in the aspect of improving the security and performance. In [32], Yum and Lee presented a general procedure to construct a CL-PKS scheme from any ID-based signature scheme. The first CL-PKS scheme was bilinear pairing based proposed by Li et al. in [33]. Whereas in [34], Au et al. presented a new security model for CL-PKS schemes which considers inside attack scenario. The first bilinear pairing free CL-PKS scheme was first proposed by He et al. in [35], which was found to be vulnerable to other attacks in [36]. In [37] a scheme ideal for IoT deployment was proposed; however, it was found to bear some flaws concerning inside attack performance by KGC in [38]. In order to provide the needed security property of anonymous authentication in [39,40] the idea of pseudonym-based authentication was employed. Despite providing privacy preservation, the limitation of overburdened TA in storing these pseudonyms for each vehicle was encountered as has shown out as the shortfall for their approach. In [41], having foreseen the problem of overburdened TA and sought to provide a solution they designed a scheme by using anonymous certificates but this was done at the expense of interactions between the infrastructures. In [42] et al., privacy protection for VANETs communications was achieved based on the technique of ID-based ring signature, but they failed to provide conditional privacy, since there was no any tracking mechanism in their algorithm [43]. Many more researchers demonstrated the need to formulate robust schemes in terms of security and privacy protection. To this cause, Bayal et al. [44] proposed an anonymous authentication scheme, however it is deemed computationally intensive in [45]. In [46], Cui et al. proposed a scheme that utilizes the methods of a cuckoo filter and binary search to facilitate batch verification for vehicular communication of V2V and V2I. He at al. [17] designed an ECC based certificate-less based signature scheme for VANETs system with batch verification feature. However, Mahmood et al. [31] states that their scheme still vulnerable to side-channel attack since some of sensitive information like TA's master private key is stored in a tamper-proof devices (TPD). A scheme in [47] uses pseudonyms instead of real identities in trying to secure VANETs communications. The scheme in [47] achieves efficiency and provides batch verification but falls short in terms of providing all security requirements like unlinkability.

3. Preliminaries

Now we will formalize the background knowledge of the building blocks for the proposed scheme. The notations used in the designed algorithm are given and described in Table 1. ECC is a public key cryptosystem based on elliptic curve theory and has an advantage for being a structure for faster and more efficient cryptosystems with robust security. ECC cryptosystems have low computational requirement hence its viable for securing resource constrained network systems that require seamless and real-time operations like the IoT and SG systems [48].

Table 1. Notations Used in the Proposed Scheme.

Symbols	**Meanings of Symbols in the Scheme**
V_i	i^{th} vehicle
$p,\ q$	Two large primes
E	Is the chosen elliptic curve, $y^3 = x^2 + ax + bmodp$ where $a, b \in Z_q^*$
$E(F_p)$	Is the prime field of an elliptic curve E order p
P	Is the generator of $E(F_p)$ with large prime order q
G	A cyclic group generated by a point P on a non-singular elliptic curve E
ID_i	A pseudo-identity of V_i such that $ID = (PID_1, PID_2, T_i)$
psk_i	Partial private key for a vehicle, V_i
(x_i, x_iP)	Secret key and public key for V_i
sk_i	Full private key for V_i
T_i	Validity period for the pseudo-identity ID_i for V_i
RID_i	A real identity for the vehicle V_i
(P_{pub}, α)	KGC's public key and master key respectively
(T_{pub}, β)	TRA's public key and master key respectively
M_i	Traffic-related message generated by V_i
t_i	Current timestamp
$H_1,\ H_2,\ H_3$	Hash function: $H_1,\ H_2 : \{0,1\}^* \rightarrow\ Z_q^*$
$\oplus$	Exclusive-OR operation
$\|\|$	concatenation

Elliptic curve: Given a prime number q, equation $y^3 = x^2 + ax + bmodp$ defines an elliptic curve over a prime field $E(F_p)$, where $p > 3, a, b \in F_q$ and satisfies $\triangle = 4a^3 + 27b^2 \neq 0modp$. The points on F_p together with the point at infinity $\mathcal{O}$ form an additive cyclic group

G. Let P be the generator point of order n, the scalar multiple operation is defined as, $nP = P + P + \cdots + P$, n times addition, where $n \in Z_q^*$, is a positive integer. So, there are a number of intractable problems in an elliptic curve group G of order n, suitable for cryptographic purposes as there is no polynomial algorithm to solve them efficiently by brute-force within probabilistic polynomial time.

Elliptic Discrete Logarithm (ECDL) Problem: Given an element $Q \in G$, the ECDL problem is to extract an element $x \in Z_q^*$, such that $Q = xP$.

Elliptic Curve Computational Diffie-Hellman (ECCDH) Problem: Given two elements $xP, yP \in G$, with unknown elements $x, y \in Z_q^*$, the ECCDH problem is to compute $Q = xyP$.

Elliptic Curve Decisional Diffie-Hellman (ECDDH) Problem: No any probabilistic polynomial time algorithm can distinguish between the tuples (P_1, xP_1, yP_1, T) and (P_1, xP_1, yP_1, xyP_1) where $P_1, T \in G$, with unknown elements $x, y \in Z_q^*$.

3.1. System Model

In terms of the communication process, the VANETs' architecture is categorized into two layers, namely the physical layer and the application layer, in which case the physical layer is comprised of the vehicles, the RSUs situated on designated points of the road. Vehicles on the roads are embodied with OBUs as a communication enabling device to connect with other vehicles, RSUs or other advanced smart city facilities. [49]. The OBU is equipped with a TPD device to secure stored sensitive information like secret key and the global positioning system (GPS). As such the vehicle is securely able to carry out advanced VANETs communications in smart cities including V2X, V2V and V2I, which are enabled by a dedicated short range communication (DSRC) protocol specifically identified as IEEE 802.11p. On the other hand, the application layers are comprised of the key generation center (KGC) and the tracing authority (TRA) application server, which are the major components undertaking the TA roles in a conditional privacy preserving VANETs based system. The design and the interplay of these main entities in the system is illustrated in Figure 1, where close range networks are facilitated by wireless communication technology such as IEEE802.11p, mid-way network communication is aided by long range communication technology coupled with high bandwidth such as WiMax. Whereas, the backbone network system is empowered by wired communication which is mostly assumed to be secure as it controlled by the public utility company. It is the wireless communication that is supposed to be secured by security algorithm that ensures authentication and integrity on all communications amongst the concerned entities. The TRA is the responsible authority for RSUs and issuing pseudo-identities to vehicles, and can do real identity revocation whenever necessary. In a like manner, the KGC is responsible for public and partial private keys' generation for both RSUs and vehicles. So in VANETs schemes, it is usually assumed that the KGC and TRA are trusted parties and hence assumed honest but curious [50]. Both KGC and TRA have sufficient computation power but the OBUs and RSUs are the one with limited computation and storage capabilities hierarchically with RSUs as most powerful one [23,29,51]. However, OBUs and RSUs are not trusted entities and therefore any communication initiative originating from them must be authenticated. Thus, this inspires the devising of security protocols for VANETs with suitable computation requirements for OBUs and RSUs.

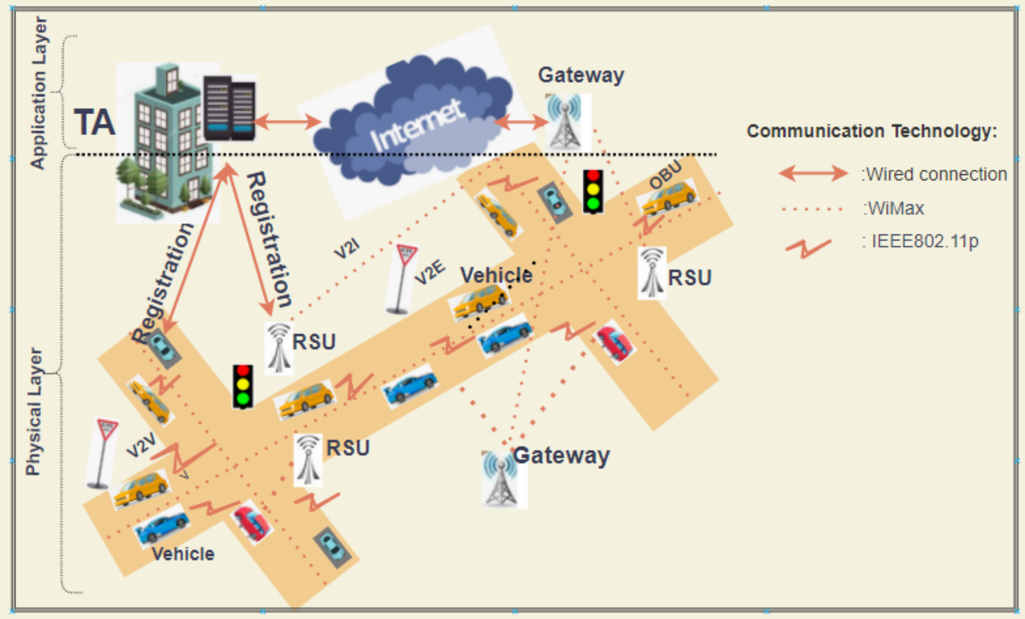

Figure 1. Two Layered Vehicular Ad hoc networks (VANETs) Architecture.

3.2. Security Model for CLAS Scheme

As proposed first in [31], in CLAS we assume two types of adversaries termed *Type 1 Adversary*, A_1, and *Type 2 Adversary*, A_2. Here, A_1 acts as a dishonest user and A_2 acts as a malicious KGC on the other hand. ***Type 1 Adversary***: A_1 adversary does not control the master key but is allowed to replace public keys at will, with any desirable value of its choice. ***Type 2 Adversary***: A_2 adversary has access and controls the master key but cannot replace the public keys of users.

The classical security model proposed in Zhang et al. [52] presents a security adversarial model for certificate-less key agreement schemes. The model is defined as a game between a challenger, C, and an adversary defined by a probabilistic polynomial-time Turing machine,$A \in \{A_1, A_2\}$. Thus, A has full control of the communication channel of all parties and parties only respond to queries from A and cannot communicate directly with each other. As a controller of the communication channel, A has powers to actively carry out the following actions, such as relaying, modifying, delaying, interleaving, deleting all the messages flowing in the system.

4. The Proposed Certificate-Less Aggregate Signature Scheme

In this section, we will explain the scheme design for VANETs integrated smart grid system titled Efficient Certificate-less Aggregate Signature Scheme with Conditional Privacy-Preservation for Vehicular Ad Hoc Networks Enhanced Smart Grid System. For easy referencing the scheme will be termed ECLAS. The proposed scheme consists of eight algorithms which are: Set-up, Pseudo-Identity Generation, Partial-Private Key Extraction, Vehicle-Key Generation, Sign, Individual Verify, Aggregate and Aggregate verify, which are explained in details as follows.

1. *Set-up*
   In this section, the TA, comprising of two mutually exclusive principle parts, which are the TRA and the KGC, will initialize the system by generating the system parameters. The TA takes as input the security parameter 1^k the algorithm outputs two large prime numbers, $p,\ q$ and a non-singular elliptic curve defined by $y^2 = x^3 + ax + b(mod\ p)$, where $a, b \in F_p$.
   - The KGC sets a point P from E and with this point generates a group G of order q. Then KGC randomly selects a number $\alpha \in Z_q^*$ and sets it as its master secret with its corresponding public key computed as $P_{pub} = \alpha P$.

- Similarly, the TRA selects a points P on E and with it generates a group G of order q. Further, TRA chooses a random number $\beta \in Z_q^*$ and computes its public key $T_{pub} = \beta P$ while setting β as its master secret key used for traceability which is known to TRA only.
- All these principle entities (TA, KGC and TRA), choose three hash functions, $H_1 : G \rightarrow Z_q^*$, $H_2 : \{0,1\}^* \rightarrow Z_q^*$ and $H_3 : \{0,1\}^* \rightarrow Z_q^*$
- Then the system public parameters $params = \{P, p, q, E, G, H_1, H_2, H_3, P_{pub}, T_{pub}\}$ are published.These $params$ are then preloaded in the tamper-proof communicating devices and RSU of the system.

2. *Pseudo-Identity-Generation\Partial-Private-Key-Extraction*
   In this phase, the TRA's responsibility is to generate pseudo-identities for the vehicles while the KGC's responsibility is to create corresponding partial private keys to the pseudo-identities. Thus, finally all vehicles under a TA are registered and preloaded with their pseudo-identities and partial private keys. By use of pseudo-identities that are closed linked to the real identities, the proposed scheme can achieve conditional privacy-preservation when it is necessary to revoke the real identity of an entity the TRA can ably do so. The process of pseudo-identity generation and linkage with partial-private-key is executed by TRA and KGC in a sequential manner as follows:
   - A vehicle, V_i, with its unique real identity denoted as RID_i selects a random number $k_i \in Z_q^*$ and calculates $PID_1 = k_i P$. Then the vehicle, V_i, sends (RID_i, PID_1) to the TRA through a secure channel.
   - The TRA first checks the RID_i, if its acceptable then it calculates, $PID_2 = RID_i \oplus H_1(\beta.PID_1||T_i||T_{pub})$, where T_i indicates the validity period of the pseudo-identity. The pseudo-identity that is used to identify a vehicle, V_i, is $ID_i = (PID_1||PID_2||T_i)$ and it is sent to the vehicle and KGC through a secure channel. During revocation TRA obtains the real identity by computing $RID_i = PID_2 \oplus H_1(\beta||T_i||T_{pub})$.
   - Upon receipt of the pseudo-identity, ID_i, KGC chooses a random number, $d_i \in Z_q^*$ and computes $Q_{ID_i} = d_i P$ and then computes the partial private key, psk_i, for the vehicle, V_i, as $psk_i = d_i + H_2(ID_i||Q_{ID_i}) \times \alpha \ mod \ p$.
   - The KGC then sends the pseudo-identity and partial private key (Q_{ID_i}, psk_i) to the vehicle, V_i, through a secure channel.

   The vehicle is able to check the authenticity of the pseudo-identity and the partial private key received from the KGC by verifying whether $psk_i.P = Q_{ID_i} + H_2(ID_i||Q_{ID_i}).P_{pub}$. The conditional privacy-preservation is enhanced in the design by combining the secret contribution from the vehicle, V_i, itself and the TRA on the other hand. It is designed in such a way that the TRA is able to revoke the real identity of the vehicle when needed to do so. At the end of it all, the pseudo-identity and the partial private key are stored in the tamper-proof devices in the vehicle.

3. *Vehicle-Key-Generation*
   The vehicle, V_i, randomly selects a secret value $x_i \in Z_q^*$ as its secret key noted as vsk_i and then calculates its corresponding public key $vpk_i = x_i.P$. Then V_i set the full private key as $sk_i = x_i + psk_i$.
4. *Sign*
   The message signature is necessary for the sake of upholding the authentication and integrity of the message to the receiver of the message who rightly does verification. The vehicle, V_i, selects one of its stored pseudo-identity, ID_i, and picks the latest timestamp, t_i. With the signing Keys (psk_i, sk_i) and the traffic related message M_i, the vehicle V_i carries out the following steps to produce a signature.
   - Selects a random number $r_i \in Z_q^*$ and computes $R_i = r_i P$.
   - Computes,
     $$h_i = H_3(M_i||ID_i||Q_{ID_i}||vpk_i||R_i||t_i) \tag{1}$$

and

$$S_i = h_i.r_i + sk_i mod p, \tag{2}$$

then, V_i computes,

$$\sigma_i = (R_i, S_i) \tag{3}$$

Here σ_i, is the computed certificate-less signature on the traffic related data M_i for latest timestamp t_i and identification ID_i.

- Then the final message that, V_i sends to nearby RSU and vehicles for verification is $(ID_i, Q_{ID_i}, vpk_i, M_i, t_i, \sigma_i)$.

These steps are routinely carried out every time, V_i sends a message to RSU.

5. *Individual Verify*
On receipt of the certificate-less signature $\sigma_i = (R_i, S_i)$ on the traffic related data M_i and timestamped at t_i signed by the vehicle along with its public key vpk_i, if the received T_i in ID_i and t_i are both valid, then the RSU performs the following procedures.

- Computes

$$h_{i,0} = H_2(ID_i || Q_{ID_i}) \tag{4}$$

and

$$h_i = H_3(M_i || ID_i || Q_{ID_i} || vpk_i || R_i || t_i) \tag{5}$$

- Verifies whether

$$S_i.P = h_i.R_i + vpk_i + Q_{ID_i} + h_{i,0}.P_{pub}, \tag{6}$$

holds or not.

The RSU accepts the certificate-less signature if the verification holds. Correctness checking works, since $P_{pub} = \alpha.P,\ Q_{ID_i} = d_i.P,\ psk_i = d_i + H_2(ID_i || Q_{ID_i}) \times \alpha \ mod p$, $R_i = r_i.P$, $sk_i = x_i + psk_i$, $h_{i,0} = H_2(ID_i || Q_{ID_i})$ and $S_i = h_i.r_i + sk_i \ mod p$. Thus the computation proceeds as follows:

$$\begin{aligned} S_i.P &= (h_i.r_i + sk_i).P \\ &= h_i.r_i.P + (x_i + psk_i)P \\ &= h_i.R_i + x_i.P + psk_i.P \\ &= h_i.R_i + vpk_i + [d_i + H_2(ID_i || Q_{ID_i})\alpha] \\ &= h_i.R_i + vpk_i + Q_{ID_i} + (h_{i,0}.\alpha)P \\ &= h_i.R_i + vpk_i + Q_{ID_i} + h_{i,0}.P_{pub}. \end{aligned}$$

However, for purposes of saving computation cost, it is recommended to do data aggregation and batch verification on the signatures from the network environment of a particular RSU.

6. *Aggregate*
Each RSU is an out-posted aggregate signature generator that collects individual certificate-less signatures into a single verifiable one. The components come from an aggregating set V on n vehicles, $\{V_1, V_2, \cdots, V_n\}$ whose corresponding pseudo-identities are $\{ID_1, ID_2, \cdots, ID_n\}$ with public keys $\{vpk, vpk_2, \cdots, vpk_n\}$ and message signature pairs (M_1, t_1, σ_1), (M_2, t_2, σ_2), $\cdots$, (M_n, t_n, σ_n), where $\sigma_i = (R_i, S_i)$ for $i = 1, 2, \cdots, n$. The RSU or an application server for the traffic control center for instance computes the sum $S = \sum_{i=i}^{n} S_i$ and output an aggregate certificate-less signature as,

$$\sigma = (R_1, S_1), (R_2, S_2), \cdots, (R_n, S_n), \tag{7}$$

for $i = 1, 2, \cdots, n$.

7. *Aggregate Verify*
   On receipt of the certificate-less aggregate signature σ from n vehicle $\{V_1, V_2, \cdots, V_n\}$ whose pseudo-identities are $\{ID_1, ID_2, \cdots, ID_n\}$ with corresponding public keys, $\{vpk, vpk_2, \cdots, vpk_n\}$ and the traffic related messages $\{M_1||t_1, M_2||t_2, \cdots, M_n||t_n\}$ then the RSU or the application server carries out the following procedures, if both T_i in ID_i and t_i are checked to be valid.

   - RSU computes
   $$h_{i,0} = H_2(ID_i||Q_{ID_i}) \tag{8}$$
   and
   $$h_i = H_3(M_i||ID_i||vpk_i||R_i||t_i) \tag{9}$$
   for $i = 1, 2, \cdots, n$
   - RSU verifies if the computation holds,
   $$S.P = \sum_{i=i}^{n} h_i.R_i + \sum_{i=i}^{n} vpk_i + \sum_{i=i}^{n} Q_{ID_i} + \sum_{i=i}^{n} h_{i,0}.P_{pub}. \tag{10}$$

   If the verification holds, then the RSU accepts the aggregate certificate-less signature. The computation is valid by the correctness check, since $P_{pub} = \alpha.P$, $Q_{ID_i} = d_iP$, $psk_i = d_i + H_2(ID_i||Q_{ID_i}) \times \ modp$, $R_i + r_iP$, $S_i = h_i.r_i + psk_i \ modp$, and $S = \sum_{i=i}^{n} S_i$, thus we obtain.

$$\begin{aligned}
S_i.P &= \sum_{i=i}^{n}(h_i.r_i + sk_i).P \\
&= \sum_{i=i}^{n} h_i.r_i.P + \sum_{i=i}^{n}(x_i + psk_i)P \\
&= \sum_{i=i}^{n} h_i.R_i + \sum_{i=i}^{n} x_i.P + \sum_{i=i}^{n} psk_i.P \\
&= \sum_{i=i}^{n} h_i.R_i + \sum_{i=i}^{n} vpk_i + \sum_{i=i}^{n}[d_i + H_2(ID_i||Q_{ID_i})\alpha]P \\
&= \sum_{i=i}^{n} h_i.R_i + \sum_{i=i}^{n} vpk_i + \sum_{i=i}^{n} Q_{ID_i} + \sum_{i=i}^{n}(h_{i,0}.\alpha)P \\
&= \sum_{i=i}^{n} h_i.R_i + \sum_{i=i}^{n} vpk_i + \sum_{i=i}^{n} Q_{ID_i} + \sum_{i=i}^{n} h_{i,0}.P_{pub}.
\end{aligned}$$

5. Analyses

From here on, we will devote to giving a formal security proof, security privacy preservation analyses and then we will present the performance evaluation of the proposed ECLAS scheme with conditional privacy-preservation for a VANETs enhanced smart grid.

5.1. Security Proof

In this section now, we will provide security proof for the proposed ECLAS scheme for VANETs. We assume the security model for CLAS schemes where there are two types of adversaries, which are *Type 1 Adversary* and *Type 2 Adversary* as demonstrated in the security model for CLAS scheme.

Theorem 1. *Under the assumption that ECDL in G is intractable, then the proposed scheme $(\epsilon, t, q_c, q_s, q_h)$, is secure against adversary 1 in random oracle model, where q_c, q_s, q_h are the **Create**, **Sign** and **Hash** queries respectively which the adversary is allowed to make.*

Proof. Suppose there is a probabilistic polynomial time adversary $\mathcal{A}_1$, we construct an algorithm $\mathcal{F}$ that solves the ECDL problem by utilizing $\mathcal{A}_1$. Assume that $\mathcal{F}$ is given an ECDL problem instance, (P, Q) to compute $x \in Z_q^*$ so that $Q = xP$. Thus, $\mathcal{F}$ chooses a challenging identity ID^* for the identity ID to answer any random queries from $\mathcal{A}_1$ as follows:

- **Set-up (**ID**) Query**: The challenger $\mathcal{F}$ selects its random numbers α^* and β^* as its master keys and has a corresponding public key as $P_{pub}^* = \alpha^* P$ and $T_{pub}^* = \beta^* P$ then sends the system parameters $\{P, p, q, E, G, H_2, H_3, P_{pub}^*, T_{pub}^*\}$ to $\mathcal{A}_1$.
- **Create (**ID**) Query**: $\mathcal{F}$ stores the hash list L_C of the tuple $(ID, Q_{ID_i}, vpk_i, psk_i, sk_i, h_2)$. Whenever an adversary $\mathcal{A}_1$ makes a query for ID, and if the ID is contained in L_C, then $\mathcal{F}$ returns $(ID, Q_{ID_i}, vpk_i, psk_i, sk_i, h_2)$ to $\mathcal{A}_1$. Then $\mathcal{F}$, execute the oracle as follows. if $ID = ID^*$, $\mathcal{F}$ randomly chooses the values $a, b, c \in Z_q^*$ and sets $Q_{ID} = a.P_{pub}^* + b.P$, $vpk_i = c.P$, $psk_i = b$, $sk_i = c$, $h_2 = H_2(ID||Q_{ID}) \leftarrow amodq$, then $\mathcal{F}$ adds (ID, Q_{ID}, h_2) to the list L_{H_2} and returns $(ID, Q_{ID_i}, vpk_i, psk_i, sk_i, h_2)$ to $\mathcal{A}_1$. as the equation $psk_i.P = Q_{ID} + h_2.P_{pub}^*$, thereby implying that the partial private key is valid.
- H_2 **Query**: Whenever an H_2 query with (ID, Q_{ID}) is made, and ID is already in the hash list L_{H_2}, then $\mathcal{F}$ reply with a corresponding h_2. On the other hand, $\mathcal{F}$ runs Create(ID) to obtain h_2 and then sends h_2 to $\mathcal{A}_1$.
- **Partial-Private-Key-Extract (**ID**) Query**: If $ID^* = ID$, then $\mathcal{F}$ aborts the game. Otherwise, $\mathcal{F}$ looks in the hash list L_C, if ID is found in the list, then $\mathcal{F}$ returns psk_i to $\mathcal{A}_1$. If ID is not in the list L_C, $\mathcal{F}$ executes Create(ID) query to obtain psk_i and sends it to $\mathcal{A}_1$.
- **Public-Key (**ID**) Query**: Upon receiving the query on ID, when ID is already in the list L_C, $\mathcal{F}$ replies with $pk = (Q_{ID}, vpk_i)$. On the other hand, $\mathcal{F}$ executes Create(ID) query to obtain (Q_{ID}, vpk_i) and sends it to $\mathcal{A}_1$.
- **Public-Key-replacement** (ID, pk') **Query**: $\mathcal{F}$ stores the hash list L_R of tuple $(ID, d_i, Q_{ID}, sk_i, vpk_i)$. When $\mathcal{A}_1$ executes the query with (ID, pk'), where $Q'_{ID} = d'.P$, $vpk'_i = x'_i.P$ and $pk\prime = (Q'_{ID}, vpk'_i)$, then $\mathcal{F}$ sets $Q_{ID} = Q'_{ID}$, $vpk_i = vpk'_i$, $psk_i = \perp$ and $x_i = x'_i$. Then the challenger $\mathcal{F}$, updates the list L_R to be $(ID, d'_i, Q'_{ID}, vpk'_i, x'_i)$.
- $H_3(ID)$ **Query**: $\mathcal{F}$ keeps the hash list L_{H_3} of the tuple $(m, ID, R, vpk_i, t, h_3)$ and if the ID queries are not in the list, $\mathcal{F}$ replies with h_3. Otherwise, it selects a random number h_3 such that $h_3 = H_3(m||ID||vpk_i||R||t)$ then add it to the list L_{H_3} and returns h_3 to $\mathcal{A}_1$
- **Sign (**ID, m**) Query**: $\mathcal{A}_1$ makes a sign query on (ID, m), once ID is on the list L_R, $\mathcal{F}$ chooses random numbers $a, b, c \in Z_q^*$, and sets $s = a$, $R = P$, $h_3 = H_3(m||ID||vpk_i||R||t)$ $\leftarrow (a - b - c)modq$ and then inserts $(m, ID, R, vpk_i, t, h_3)$ to the list L_{H_3}. The resultant signature is (R, s), and if ID is not in the list L_R, then $\mathcal{F}$ acts according to scheme's procedure.

□

As a result, $\mathcal{A}_1$ produces a forged signature $\sigma = (R, s_{\{1\}})$ on the message (ID, m) which passes verification process. If $ID \neq ID^*$, $\mathcal{F}$ aborts the process. $\mathcal{F}$ keeps on challenging $\mathcal{A}_1$ up until it responds to the H_3 query. $\mathcal{A}_1$ will be prompted to generate another valid signature $\sigma = (R, s_{\{2\}})$ by using the same R. Thus we have:

$$s_{\{i\}}.P = h_{3\{i\}}.R + vpk_i + Q_{ID} + h_2.P_{pub}^*, \tag{11}$$

where $i = 1, 2$.

By solving the two linear equations we obtain the value of r by

$$\frac{s_2 - s_1}{h_{\{2\}} - h_{\{1\}}}, \tag{12}$$

similarly, with continuous querying, H_2 will allow computation of x.

Probabilistic Analysis: The simulation of Create(ID) queries fails when the random oracle assignment $H_2(ID||Q_{ID})$ causes inconsistency with the probability of at most $\frac{q_h}{q}$. The probability of successful simulation of q_c times is at least $(1-\frac{q_h}{q})^{q_c} \geq 1-(\frac{q_h q_c}{q})$. Similarly, the simulation is q_h successful with the probability of at least $(1-\frac{q_h}{q})^{q_h} \geq (1-\frac{q_h^2}{q})$ and $ID = ID^*$ with the probability of $\frac{1}{q_c}$. Thus, in overall the probability of successful simulation is

$$(1-\frac{q_h q_c}{q})(1-\frac{q_h^2}{q})(\frac{1}{q_c})\epsilon. \quad (13)$$

Theorem 2. *Under the assumption that ECDL in G is intractable, then the proposed scheme* $(\epsilon, t, q_c, q_s, q_h)$*, is secure against adversary 2 in random oracle model, where* q_c, q_s, q_h *are the* ***Create****,* ***Sign*** *and* ***Hash*** *queries respectively which the adversary is allowed to make.*

Proof. Suppose there is a probabilistic polynomial time adversary $\mathcal{A}_2$, we construct an algorithm $\mathcal{F}$ that solves the ECDL problem by utilizing $\mathcal{A}_2$. Assume that $\mathcal{F}$ is given a ECCDH problem instance, (P, Q) to compute $x, y \in Z_q^*$ so that $Q = xyP$. Thus, $\mathcal{F}$ chooses an challenging identity ID^* for the identity ID to answer any random queries from $\mathcal{A}_2$ as follows:

- **Set-up (**ID**) Query**: The challenger $\mathcal{F}$ selects its random numbers α^* and β^* as its master keys and has a corresponding public key as $P_{pub}^* = \alpha^* P$ and $T_{pub}^* = \beta^* P$ then sends the system parameters $\{P, p, q, E, G, H_2, H_3, P_{pub}^*, T_{pub}^*\}$ to $\mathcal{A}_2$.
- **Create (**ID**) Query**: $\mathcal{F}$ stores the hash list L_C of the tuple $(ID, Q_{ID_i}, vpk_i, psk_i, sk_i, h_2)$. Whenever an adversary $\mathcal{A}_2$ makes a query for ID, and if the ID is contained in L_C, then $\mathcal{F}$ returns $(ID, Q_{ID_i}, vpk_i, psk_i, sk_i, h_2)$ to $\mathcal{A}_2$. If $ID = ID^*$, $\mathcal{F}$ randomly selects $a, b \in Z_q^*$ and computes $Q_{ID} = aP, vpk_i = Q, h_2 = H_2(ID||Q_{ID}) \leftarrow b, psk_i = a + x.h_2$, $sk_i = \perp$. If $ID =\neq ID^*$, $\mathcal{F}$, randomly selects $a, b, c \in Z_q^*$ and computes $Q_{ID} = a.P$, $vpk_i = b.P$, $h_2 = H_2(ID||Q_{ID}) \leftarrow c$, $psk_i = a + x.h_2$, $sk_i = b$. Then $\mathcal{F}$, responds to the query with $(ID, Q_{ID_i}, vpk_i, psk_i, sk_i, h_2)$ and then appends (ID, Q_{ID}, h_2) to the hash list L_{H_2}.
- H_2 **Query**: Whenever an adversary $\mathcal{A}_2$ makes an H_2 query with (ID, Q_{ID}), and ID is already in the hash list L_{H_2}, then $\mathcal{F}$ reply with a corresponding h_2. On the other hand, $\mathcal{F}$ runs Create(ID) to obtain h_2 and then sends h_2 to $\mathcal{A}_2$.
- **Partial-Private-Key-Extract (**ID**) Query**: Upon receipt of the query on ID, $\mathcal{F}$ verifies from the hash list L_C, if ID is found to be in the hash list $\mathcal{F}$ returns psk_i to $\mathcal{A}_2$. If ID is not in the hash list, L_C, $\mathcal{F}$ executes Create(ID) query to obtain psk_i and sends it to $\mathcal{A}_2$.
- **Public-Key (**ID**) Query**: Upon receipt of query on ID, when ID is already in the list L_C, $\mathcal{F}$ replies with $pk = (Q_{ID}, vpk_i)$. On the other hand, $\mathcal{F}$ executes Create(ID) query to obtain (Q_{ID}, vpk_i) and sends it to $\mathcal{A}_2$.
- **Secret-Key-Extract** (ID) **Query**: On receipt of the queries from $\mathcal{A}_2$, if $ID = ID^*$, $\mathcal{F}$ stops the simulation. While, if ID is already in the list L_C, then $\mathcal{F}$ reply with sk_i. Whereas if, ID is not in the list L_C, $\mathcal{F}$ executes Create(ID) query to obtain $(ID, Q_{ID}, vpk_i, psk_i, sk_i, h_2)$ and sends sk_i to $\mathcal{A}_2$.
- $H_3(ID)$ **Query**: $\mathcal{F}$ keeps the hash list L_{H_3} of the tuple $(m, ID, R, vpk_i, t, h_3)$ and if the ID queries are in the list, $\mathcal{F}$ replies with h_3. Otherwise, it selects a random number h_3 such that $h_3 = H_3(m||ID||vpk_i||R||t)$ then add it to the list L_{H_3} and returns h_3 to $\mathcal{A}_2$
- **Sign (**ID, m**) Query**: As $\mathcal{A}_2$ makes a sign query on (ID, m), once $ID \neq ID^*$, $\mathcal{F}$ acts according to protocol flow. Otherwise, $\mathcal{F}$ randomly chooses the values $a, b, f \in Z_q^*$ and sets $s = a, h_3 = H_3(m||ID||vpk_i||R||t) \leftarrow f, R = h_3^{-1}(bP_{pub}^* - Q)$, and returns the signature (R, s). If the verification, $s.P = h_3.R + Q_{ID} + vpk_i + h_2.P_{pub}^*$, holds then the signature is valid.

□

As a result, $\mathcal{A}_2$ produces a forged signature $\sigma = (R, s_{\{2\}})$ on the message (ID, m) which passes verification process. If $ID \neq ID^*$, $\mathcal{F}$ aborts the process. $\mathcal{F}$ keeps on challenging $\mathcal{A}_2$ up until it responds to the H_3 query. $\mathcal{A}_2$ will be prompted to generate another valid signature $\sigma = (R, s_{\{2\}})$ by using the same R. Thus we have:

$$s_{\{i\}}.P = h_{3\{i\}}.R + vpk_i + Q_{ID} + h_2.P^*_{pub}, \tag{14}$$

$$s_{\{i\}} = h_{3\{i\}}.r + y + d_i + h_2.x, \tag{15}$$

where $i = 1, 2$.

By solving the two linear equations involving r and y as variables, we can derive the value of y as an output of ECDL problem.

5.2. Security and Privacy-Preservation Analyses

This part discusses the security and privacy-preservation features satisfied by the proposed scheme, specifically this is in respect to anonymity (identity privacy), message authentication, data integrity, traceability, unlinkability and resistance to attacks.

- Anonymity: In the proposed scheme the vehicle's identification ID_i is not the real identification RID_i, but rather a pseudo-identity as offered by the TRA for purposes of achieving conditional privacy of the vehicle in VANETs. The only way for an adversary or any malicious party to obtain the real identity it by computing $RID_i = ID_i \oplus H_1(\beta.PID_1||T_i||T_{pub})$. Without knownledge of the TRA's master private key β, no other party can know the vehicle's real identity RID_i, since it requires β to calculate $H_1(\beta.PID_1||T_i||T_{pub})$. This manipulation is infeasible for an adversary to achieve since the extraction of β from $T_{pub} = \beta.P$, involves an intractable ECDL problem. Therefore, these claims ascertain the satisfaction of user identity privacy-preservation.
- Message Integrity and Authentication: By virtue of signing a message before broadcasting, the legitimate user's authenticity is verified. Based on the ECDLP assumption the authenticity and integrity of the message $(ID_i, Q_{ID_i}, vpk_i, M_i, t_i, \sigma_i)$ is upheld by verifying the computation $S_i.P = h_i.R_i + vpk_i + Q_{ID_i} + h_{i,0}.P_{pub}$. Since $h_i = H_3(M_i||ID_i||Q_{ID_i}||vpk_i||R_i||t_i)$ and $h_{i,0} = H_2(ID_i||Q_{ID_i})$, no malicious party can forge $\sigma_i = (R_i, S_i)$ which achieves the maessage integrity and authentication of which needs knoweledge of full private key $sk_i = x_i + psk_i$ in its formulation.
- Traceability: Although the vehicle is identified by a pseudonym, in necessary circumstances the real identity of a particular vehicle can be mapped back from the pseudonym. For instance, the pseudo-identity of a vehicle is $ID_i = (PID_1||PID_2||T_i)$ and the TRA can revoke the real identity by calculating $PID_2 = RID_i \oplus H_1(\beta.PID_1||T_i||T_{pub})$. As such, once a vehicle is flagged as questionable the TRA is able to trace its true identity and thereby carrying out whatever necessary procedures to curb any kind of malpractice. Once this is done the TRA records the real identity RID_i on the revocation list of the system and as a result the vehicle cannot use its corresponding pseudo-identity ID_i.
- Unlinkability: The message transmitted $(ID_i, Q_{ID_i}, vpk_i, M_i, t_i, \sigma_i)$ from a vehicle V_i to others has the component $PID_1 = k_i P$, where $k_i \in Z^*_q$ is random, that is randomly generated for any particular message transmitted. Since the PID_1 is also a component for pseudo-identity generation, it means the randomness in PID_1 results in the randomness of the publicized pseudo-identity ID_i, hence, any two individual captures of the pseudo-identity ID_i for V_i stills seem random and unrelated to the real identity RID_i, in the eyes of eavesdroppers. So by virtue of the identification being anonymous and distinct any captured signatures cannot be linked to previously captured identity nor to a particular true signer. Thus, any communication is seen as random and new in the plying eyes of an adversary and has no any relationship to previous communications for an eavesdropper to learn any useful information from such communication.

- Resistance to Attacks: At this point we will present a demonstration of how the proposed ECLAS scheme can resist the main common attacks such as—replay attack, modification attack, impersonation attack, and stolen verifier attack.
  - Replay Attack Resilience: In the message $(ID_i, Q_{ID_i}, vpk_i, M_i, t_i, \sigma_i)$ the t_i in the message helps in checking replay attacks. The recipients, RSUs or vehicles will have to check the freshness of the message, and once the timestamp is invalid the message is discarded. As such the proposed scheme, ECLAS, could resist against replay attack.
  - Modification Attack Resilience: In the scheme a valid message $(ID_i, Q_{ID_i}, vpk_i, M_i, t_i, \sigma_i)$ has a valid digital conditional anonymous signature (ID_i, σ_i). Any modification to the message $(ID_i, Q_{ID_i}, vpk_i, M_i, t_i, \sigma_i)$ can be detected during verification $S_i.P = h_i.R_i + vpk_i + Q_{ID_i} + h_{i,0}.P_{pub}$ which simultaneously authenticates the sender, V_i, and the TA side of TRA and KGC. Therefore, the proposed ECLAS scheme stands against modification attack.
  - Impersonation Attack Resilience: It is not feasible for an attacker to launch a successful impersonation on the message $(ID_i, Q_{ID_i}, vpk_i, M_i, t_i, \sigma_i)$ of which can pass verification as if it was generated by a legal user V_i. However, it is impossible for an attacker to obtain the KGC's master key α and the users private key x_i from the publicly accessible parameters as it will involve solving the intractable problems of ECDLP and ECCDHP from $vpk_i = x_iP$ and $P_{pub} = \alpha P$.
  - Stolen Verifier Table Attack Resilience: In the proposed ECLAS scheme, both the TA side, which comprises of TRA and KGC and the user side, which comprises of RSUs and OBUs on the vehicle do not require a check list. This implies resistance against stolen verification table attack as it means the table can not be stolen.
  - Key-Escrow Resilience: Although the TAs side has access to the master keys used for generating the user's partial private key, still more neither TRA nor KGC can generate a valid signature $\sigma_i = (R_i, Si)$ for a valid message $(ID_i, Q_{ID_i}, vpk_i, M_i, t_i, \sigma_i)$. This is due to the fact that, the vehicle adds a secret value x_i to the partial private key psk_i when computing its full private key $sk_i = x_i + d_i + H_2(ID_i||Q_{ID_i})\alpha$, which is used for signing messages. To this effect although TRA knows the master key β and KGC knows the master key α for the systems, they cannot forge messages to masquerade as V_i illegally. Thus, the proposed ECLAS scheme withstands the key escrow attacks.

Now we will present a comparison analysis of ECLAS with recent related works in terms of security features satisfied. In Table 2 the results of the comparison is provided with the features coded as, SF-1, SF-2, SF-3, SF-4, SF-5, SF-6 to denote, integrity and authentication, anonymity, traceability and revocability, unlinkability, key escrow problem and resistance to common attacks respectively. In the Table 2 the symbol ✓denotes the satisfaction whereas ✗, denotes not satisfaction of the security feature. As shown by the comparison table, the schemes in [47,53,54] fall short from fulfilling some of the features.

Table 2. Comparison Analysis of Security Features Satisfied.

Security Feature	**Alazzawi et al. [47]**	**Bayat et al. [53]**	**Malhi et al [54]**	**ECLAS**
SF-1	✓	✓	✗	✓
SF-2	✓	✓	✓	✓
SF-3	✓	✓	✓	✓
SF-4	✗	✗	✓	✓
SF-5	✗	✗	✗	✓
SF-6	✓	✗	✗	✓

5.3. Performance Evaluation

In this section, we will present the performance analysis of the proposed ECLAS scheme in terms of comparable feature with related research on the fields that gives merit to the proposed scheme. As such, performance comparison features are discussed in terms of computation cost analysis and communication cost analysis. We will assess the performance evaluation of the proposed work in terms of computation cost comparison against other related works by adopting the method presented in [17]. In [17] bilinear pairing on an 80 bits security parameter length is created as : $G_1 \times G_2 \rightarrow G_T$. Here we consider G_1 as an additive group of order q defined on a super-singular elliptic curve $E : y^2 = x^3 + xmodp$ of embedding degree of 2. The recommended security parameter length for q and solinas prime number p are taken as 512 bits and 160 bits, respectively.

For convenience, we will define the notations for execution time for different cryptographic computations in the schemes under discussion as portrayed in Table 3. We borrow the execution times directly from [17], which was evaluated using the MIRACL cryptographic library, to assess the efficiency of schemes. Operations which are very light like addition operation in Z_q^* and the multiplication operation in Z_q^* will not be considered.

Table 3. Execution Times of Cryptographic Operations.

Operations	T_{bp}	$T_{bp.m}$	$T_{bp.sm}$	$T_{bp.a}$	T_H	$T_{e.m}$	$T_{e.sm}$	$T_{e.a}$	T_h
Times (ms)	4.211	1.709	0.0535	0.0071	4.406	0.4420	0.0138	0.0018	0.0001

The notation for various computation operations are as follows.

T_{bp}: Denotes execution time for bilinear pairing operation defined as, $e(P, Q)$, where $P, Q \in G_1$

$T_{bp.m}$: Denotes execution time for scalar multiplication operation $x.P$, that is related to pairing operation defined as $e(P, Q)$, where $P, Q \in G_1$, and $x \in Z_q^*$

$T_{bp.sm}$: Denotes execution time for small scalar multiplication operation, $v_i.P$, that is related to pairing operation $e(P, Q)$, where $P, Q \in G_1$ and $v_i \in [1, 2^t]$ is a small random integer, for a small predefined integer t.

$T_{bp.a}$: Denotes execution time for point addition in bilinear pairing operation $e(P, Q)$, such that $R = P + Q$, where $R, P, Q \in G_1$

T_H: Denotes execution time for map-to-point hash function operation related to pairing operation $e(P, Q)$, where $P, Q \in G_1$.

$T_{e.m}$: Denotes execution time for scalar multiplication operation, $x.P$, over ECC group, where $P \in G$ and $x \in Z_q^*$.

$T_{e.sm}$: Denotes execution time for small scalar multiplication operation, $v_i.P$, for small exponent test, where $P \in G$ and $v_i \in [1, 2^t]$ is a small random integer, for a small predefined integer t.

$T_{e.a}$: Denotes execution time for point addition operation over an elliptic curve group, $R = P + Q$, where $R, P, Q \in G$.

T_h: Denotes execution time for one hash function operation.

5.3.1. Computation Cost Analysis

In this section, we give a formal security proof on the proposed certificate-less signature scheme. While using the computation execution times for various dominant time-consuming cryptographic operations summarized in Table 3, we carry out a computation analysis of related CLAS schemes [2,13,23,27,55] in terms of the three phases of message signing, individual verify and aggregate verify overhead in RSU. The observation is clear that our proposed scheme, ECLAS, has better computation performance to related works from Table 4. In [27], to generate a signature a vehicle carries out three scalar multiplication, $3T_{e.m}$, over an elliptic curve. This means the computation cost for signing is $3T_{e.m} \approx 1.326\ ms$. Whilst for verifying a signature, three bilinear pairings, one scalar multiplication over an elliptic curve and one map-to-point hash function operations, are required.

Thus, individual verification needs $2T_{bp} + T_{e.m} + T_H \approx 17.481$ ms. In aggregate verification phase, three bilinear pairings, n scalar multiplication over elliptic curve and n map-to-point hash function operations are required, $2T_{bp} + nT_{e.m} + nT_H \approx 12.633 + 4.4198n$ ms. In the proposed ECLAS scheme, for signature generation a vehicle requires two scalar multiplication with respect to elliptic curve and one hash function operation, $2T_{e.m} + T_h$, amounting to the computation load of $2T_{e.m} + T_h \approx 0.8841$ ms. For individual signature verification, ECLAS, similarly requires two scalar multiplication with respect to elliptic curve and one hash function operation, $2T_{e.m} + T_h$, amounting to the computation load of $2T_{e.m} + T_h \approx 0.8841$ ms. Whereas for aggregate signature verification, ECLAS requires $2n$ scalar multiplication with respect to elliptic curve and n hash function operation, $2nT_{e.m} + nT_h$, yielding computation cost of $2nT_{e.m} + nT_h \approx 0.8841n$ ms. in a similar manner, the computation cost for other relevant comparable schemes [2,13,23,55] can be calculated. Based on the generated summary results of computation cost comparison done in Table 4 and the visual representation done given in Figure 2 we make conclusion on the performance of ECLAS. It is clear that the proposed ECLAS scheme has all over computation efficiency compared to the rest of the scheme except [13], and although it has a slightly lower signing computation overhead it was found to have security flaws in [23], whereas the proposed scheme satisfies the security requirements and withstands KGC escrow property.

Table 4. Comparison of Computation Costs for Related Certificate-less aggregate signature (CLAS) Schemes in ms.

Schemes	Message Signing	Individual Verify	Aggregate Verify
Horng et al. [27]	$3T_{e.m} \approx 1.326$ ms	$3T_{bp} + T_{e.m} + T_H$ ≈ 17.481 ms	$3T_{bp} + nT_{e.m} + nT_H$ $\approx 12.633 + 4.4198n$ ms
Cui et al. [13]	$T_{e.m} + T_{e.a} + T_h$ ≈ 0.4439 ms	$3T_{e.m} + 2T_{e.a} + 2T_h$ ≈ 1.3298 ms	$(n+2)T_{e.m} + 4nT_{e.a}$ $+nT_H + nT_h$ $\approx 6.2973n$ ms
Xiong et al. [55]	$3T_{bp.m} + 2T_{bp.a} + T_h$ ≈ 5.1413 ms	$3T_{bp} + 2T_{bp.m} + T_{bp.a}$ $+T_H + T_h$ ≈ 19.2262 ms	$3T_{bp} + 2nT_{bp.m} + nT_{bp.a}$ $+nT_H + nT_h$ $\approx 12.633 + 7.8312n$ ms
Tzeng et al. [2]	$3T_{bp.m} + T_H$ ≈ 9.533 ms	$2T_{bp} + T_{bp.m}$ ≈ 10.131 ms	$2nT_{bp} + nT_{bp.m}$ $\approx 10.131n$ ms
Kamil et al. [23]	$3T_{e.m} + 2T_{e.a} + 3T_h$ ≈ 1.3297 ms	$2T_{e.m} + T_{e.a} + T_h$ ≈ 0.8859 ms	$2nT_{e.m} + nT_{e.a} + nT_h$ $\approx 0.8859n$ ms
ECLAS	$2T_{e.m} + T_h$ ≈ 0.8841 ms	$2T_{e.m} + T_h$ ≈ 0.8841 ms	$2nT_{e.m} + nT_h$ $\approx 0.8841n$ ms

For simplicity sake, by regarding equal computation capabilities for signing and verifying then we can lump up the computation load that is incurred in message signing and individual verifying for a single signature. As such, the overall load for Horng et al. [27] comes up to $(1.326 + 17.481)$ $ms = 18.807$ ms and for Cui et al. [13] the overall load is $(0.4439 + 1.3298)$ $ms = 1.7737$ ms. Proceeding in this manner for the rest of the schemes, in Xiong et al. [55], Tzeng et al. [2], Kamil et al. [23] the overall computation loads are; 24.3675 ms, 19.664 ms, 2.1887 ms respectively. Subsequently, ECLAS has an overall computation load of 1.7682 ms, which is better than the rest as shown in Figure 2.

The relationship of verification time delay for particular number of aggregate signatures that RSU takes to compute for the schemes [2,13,23,27,55] is portrayed in the Figure 3.

As a requirement in VANETs, vehicles have to broadcast their messages every 100–300 ms, thus it entails that an RSU or AS can receive about 180 messages every 300 ms. Therefore, in one second an RSU is expected to verify about 600–2000 messages [23]. In Figure 3, it endeavors to illustrate the time it takes to do batch verification for 2000 signatures. Thus, the comparative analysis shows that the proposed scheme has less verification time delay for *n* signature aggregation and the number of signatures has a direct proportion linear relationship to the verification delay.

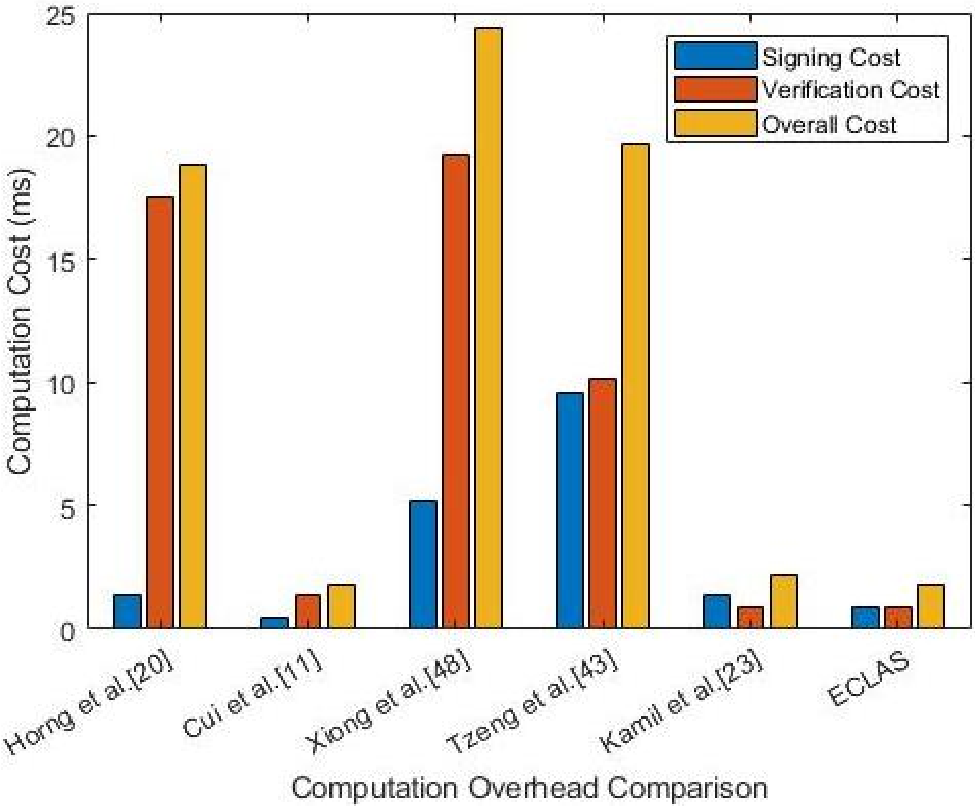

Figure 2. Computation Cost Comparison Per Unit.

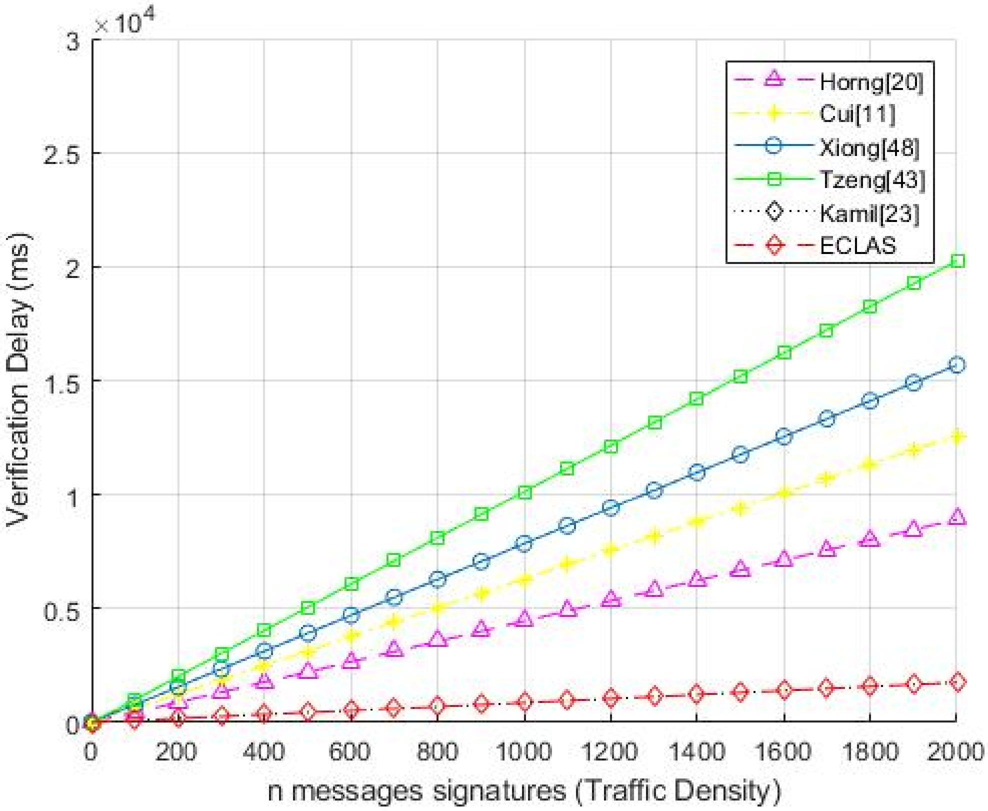

Figure 3. Verification Time Delays and Number of Signatures Relationship.

5.3.2. Communication Cost Analysis

In this part now, we will present the communication overhead of the proposed scheme against the related schemes [2,13,23,27,55] by borrowing experiment results from [17] to account for transmission cost for sending packets from vehicle to RSUs in V2I or V2V communication in VANETs, the sizes of elements in G_1 and G are 128 bytes and 40 bytes respectively. In addition, the elements in Z_q^*, the hash function value and timestamps are of the sizes 20 bytes, 20 bytes and 4 bytes respectively. We will consider the message traffic load for signatures only.

In [27], the vehicle broadcast the message $(ID_i, vpk_i, M_i, t_i, \sigma_i = (R_i, S_i))$ to RSUs, where $ID_i, vpk_i, R_i, S_i \in G$ and t_i is a timestamp. Therefore, the communication overhead is $3 \times 40 + 4 = 124$ bytes. In [13] the vehicle sends the message $(ID_i, vpk_i, Q_{ID_i}, \sigma_i = (R_i, S_i), t_i)$ to RSUs or AS, where $ID_i, vpk_i, Q_{ID_i}, R_i \in G$, $S_i \in Z_q^*$ and t_i is the timestamp. Thus, the communication load on the network is $4 \times 40 + 20 + 4 = 184$ bytes. In [55], the vehicle sends $(ID_i, m_i, upk_i, signature(U_i, V_i))$ to RSU, which requires the bandwidth size of $4 \times 40 + 20 + 4 = 184$ bytes. Whereas, in [54] the message sent from a vehicle to RSU is $(PS_j, PS1_j, P_i, PP_i, \sigma_i = (U_i, V_{ijk}))$, where $PS_j, PS1_j, P_i, PP_i, U_i, V_{ijk} \in G$. Therefore, the communication overhead is $6 \times 128 = 768$ bytes. In the proposed, ECLAS, scheme a vehicle sends traffic related signed message $(ID_i, Q_{ID_i}, vpk_i, M_i, t_i, \sigma_i)$ to the verifier where $ID_i \in G$. Therefore, the total communication overhead is $4 \times 40 + 20 + 4 = 184$ bytes. The proposed scheme has less communication overhead load than [27,54] and is on a par with the schemes in [46,51,55] as outlined in Table 5.

Table 5. Communication Overhead Summary.

Schemes	Sending of One Signature Message	Sending of n Signature Message
Horng et al. [27]	644 bytes	644n bytes
Cui et al. [13]	184 bytes	184n bytes
Xiong et al. [55]	184 btes	184n bytes
Malhi [54]	768 bytes	768n bytes
Kamil et al. [23]	184 bytes	184n bytes
ECLAS	184 bytes	184n bytes

However, these comparable works are found to be insecure in different aspects, like in [13], which so far has a decent efficient output, it was discovered that the scheme is insecure in [23,27].

6. Conclusions

In this paper, we presented an efficient certificate-less signature scheme with conditional privacy preservation for VANETs enhanced smart grid system that is based on elliptic curve cryptography and it provides user anonymity. The proposed work also removes the inherently key escrow problem associated with identity based cryptography by means of introducing a derivation of a full private key by the vehicle itself. Security proof under the random oracle model approach shows that the proposed scheme is secure by virtue of satisfying all the security requirements for VANETs. In this scheme certificate-less property is achieved without key escrow problem since the signature is derived by using a vehicle full private key which is not known by the KGC. Furthermore, the scheme does not require the computation intensive bilinear pairing and map-to-point hash function operations but rather is just based on less intensive operation over elliptic curve group in the design, hence achieving efficient computation cost. Even the communication overhead is within bounds with comparable schemes whilst achieving higher security merits. Thus, it is a comparatively efficient certificate-less aggregate signature scheme ideal for VANETs communications.

Author Contributions: Scheme design, methodology and the mathematical formal analysis and performance evaluation of the scheme, T.F.V.; supervision and validation D.H. and C.M. Visualization and review, original draft writing, T.F.V.; consolidation and corrections C.M.; moderation. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by World Bank at African Center of Excellence in Internet of Things (ACEIoT), of the University of Rwanda.

Acknowledgments: This research was possible because of the financial support from the World Bank, at the ACEIoT (African Center of Excellence in Internet of Things) which resides at the College of Science and Technology, Nyarugenge Campus, in Kigali, of the University of Rwanda.

Conflicts of Interest: The authors declare that there is no conflict of interest that may interfere with the research results, interpretation or whatsoever else in contrast to research discipline and conduct. The funders had no role in the design of the study; analysis or interpretation nor dictated anything for their interest, but rather the research proceeded naturally and innocently.

Abbreviations

The following abbreviations are used in this manuscript:

TTP	Trusted Third Party
VANETs	Vehicular Ad hoc Networks
MANETs	Mobile Ad hoc Networks
ECDL	Elliptic Curve Discrete Logarithm
CLAS	Certificate-less Signature Scheme

RSUs	Road Sign Units
OBUs	Onboard Units
EVs	Electric Vehicles
ECC	Elliptic Curve Cryptography
TA	Trusted Authority
PKI	Public Key Infrastructure
ITS	Intelligent Transport System
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
V2G	Vehicle-to-Grid
V2E	Vehicle-to-Everything
ECCDH	Elliptic Curve Computational Diffie-Hellman
ECDL	Elliptic Curve Discrete Logarithm
ECDDH	Elliptic Curve Decisional Diffie-Hellman
WSN	Wireless Sensor Network
IoT	Internet of Things
CRL	Certificate Revocation List
CL-PKS	Certificateless Public Key Signature
KGC	Key Generation Center
TRA	Tracing Authority
TPD	Tamper-Proof Device

References

1. Li, J.; Choo, K.K.R.; Zhang, W.; Kumari, S.; Rodrigues, J.J.; Khan, M.K.; Hogrefe, D. EPA-CPPA: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *Veh. Commun.* **2018**, *13*, 104–113. [CrossRef]
2. Tzeng, S.F.; Horng, S.J.; Li, T.; Wang, X.; Huang, P.H.; Khan, M.K. Enhancing security and privacy for identity-based batch verification scheme in VANETs. *IEEE Trans. Veh. Technol.* **2015**, *66*, 3235–3248. [CrossRef]
3. Fotros, M.; Rezazadeh, J.; Sianaki, O.A. A Survey on VANETs Routing Protocols for IoT Intelligent Transportation Systems. In Proceedings of the Workshops of the International Conference on Advanced Information Networking and Applications, Caserta, Italy, 15–17 April 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 1097–1115.
4. Lee, E.K.; Gerla, M.; Pau, G.; Lee, U.; Lim, J.H. Internet of Vehicles: From intelligent grid to autonomous cars and vehicular fogs. *Int. J. Distrib. Sens. Netw.* **2016**, *12*, 1550147716665500. [CrossRef]
5. Hayes, M.; Omar, T. End to End VANET/IoT Communications A 5G Smart Cities Case Study Approach. In Proceedings of the 2019 IEEE International Symposium on Technologies for Homeland Security (HST), Woburn, MA, USA, 5–6 November 2019; pp. 1–5.
6. Rigas, E.S.; Ramchurn, S.D.; Bassiliades, N. Managing electric vehicles in the smart grid using artificial intelligence: A survey. *IEEE Trans. Intell. Transp. Syst.* **2014**, *16*, 1619–1635. [CrossRef]
7. Alshahrani, S.; Khalid, M.; Almuhaini, M. Electric vehicles beyond energy storage and modern power networks: Challenges and applications. *IEEE Access* **2019**, *7*, 99031–99064. [CrossRef]
8. Zhao, Z.; Zhao, B.; Xia, Y. Research on power grid load after electric vehicles connected to power grid. In Proceedings of the 2015 8th International Conference on Grid and Distributed Computing (GDC), Jeju, Korea, 25–28 November 2015; pp. 36–39.
9. Wang, J.; Liu, C.; Ton, D.; Zhou, Y.; Kim, J.; Vyas, A. Impact of plug-in hybrid electric vehicles on power systems with demand response and wind power. *Energy Policy* **2011**, *39*, 4016–4021. [CrossRef]
10. Wang, Q.; Liu, X.; Du, J.; Kong, F. Smart charging for electric vehicles: A survey from the algorithmic perspective. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1500–1517. [CrossRef]
11. Du, J.; Ma, S.; Wu, Y.C.; Poor, H.V. Distributed hybrid power state estimation under PMU sampling phase errors. *IEEE Trans. Signal Process.* **2014**, *62*, 4052–4063. [CrossRef]
12. Song, J.; Yang, F.; Choo, K.K.R.; Zhuang, Z.; Wang, L. SIPF: A secure installment payment framework for drive-thru internet. *ACM Trans. Embed. Comput. Syst. (TECS)* **2017**, *16*, 1–18. [CrossRef]
13. Cui, J.; Zhang, J.; Zhong, H.; Shi, R.; Xu, Y. An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks. *Inf. Sci.* **2018**, *451*, 1–15. [CrossRef]
14. Sharma, S.; Kaul, A. VANETs Cloud: Architecture, Applications, Challenges, and Issues. In *Archives of Computational Methods in Engineering*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 1–22.
15. Shrestha, R.; Bajracharya, R.; Nam, S.Y. Challenges of future VANET and cloud-based approaches. *Wirel. Commun. Mob. Comput.* **2018**, *2018*. [CrossRef]
16. Whaiduzzaman, M.; Sookhak, M.; Gani, A.; Buyya, R. A survey on vehicular cloud computing. *J. Netw. Comput. Appl.* **2014**, *40*, 325–344. [CrossRef]

17. 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]
18. Al-shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. An efficient identity-based conditional privacy-preserving authentication scheme for secure communication in a vehicular ad hoc network. *Symmetry* **2020**, *12*, 1687. [CrossRef]
19. Sari, A.; Onursal, O.; Akkaya, M. Review of the security issues in vehicular ad hoc networks (VANET). *Int. J. Commun. Netw. Syst. Sci.* **2015**, *8*, 552. [CrossRef]
20. Cheng, L.; Wen, Q.; Jin, Z.; Zhang, H.; Zhou, L. Cryptanalysis and improvement of a certificateless aggregate signature scheme. *Inf. Sci.* **2015**, *295*, 337–346. [CrossRef]
21. Qu, F.; Wu, Z.; Wang, F.Y.; Cho, W. A security and privacy review of VANETs. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 2985–2996. [CrossRef]
22. Mansour, M.B.; Salama, C.; Mohamed, H.K.; Hammad, S.A. VANET security and privacy-an overview. *Int. J. Netw. Secur. Its Appl. (IJNSA)* **2018**, *10*.
23. Kamil, I.A.; Ogundoyin, S.O. An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks. *J. Inf. Secur. Appl.* **2019**, *44*, 184–200. [CrossRef]
24. Ali, I.; Li, F. An efficient conditional privacy-preserving authentication scheme for Vehicle-To-Infrastructure communication in VANETs. *Veh. Commun.* **2020**, *22*, 100228. [CrossRef]
25. Zhang, C.; Lin, X.; Lu, R.; Ho, P.H.; Shen, X. An efficient message authentication scheme for vehicular communications. *IEEE Trans. Veh. Technol.* **2008**, *57*, 3357–3368. [CrossRef]
26. Lu, R.; Lin, X.; Zhu, H.; Ho, P.H.; Shen, X. ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. In Proceedings of the IEEE INFOCOM 2008-The 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008; pp. 1229–1237.
27. Horng, S.J.; Tzeng, S.F.; Huang, P.H.; Wang, X.; Li, T.; Khan, M.K. An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks. *Inf. Sci.* **2015**, *317*, 48–66. [CrossRef]
28. Boneh, D.; Gentry, C.; Lynn, B.; Shacham, H. Aggregate and verifiably encrypted signatures from bilinear maps. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, 4–8 May 2003; Springer: Berlin/Heidelberg, Germany, 2003; pp. 416–432.
29. Li, K.; Au, M.H.; Ho, W.H.; Wang, Y.L. An efficient conditional privacy-preserving authentication scheme for vehicular ad hoc networks using online/offline certificateless aggregate signature. In Proceedings of the International Conference on Provable Security, Cairns, QLD, Australia, 1–4 October 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 59–76.
30. Taha, M.M.; Hasan, Y.M. VANET-DSRC protocol for reliable broadcasting of life safety messages. In Proceedings of the 2007 IEEE International Symposium on Signal Processing and Information Technology, Giza, Egypt, 15–18 December 2007; pp. 104–109.
31. Al-Riyami, S.S.; Paterson, K.G. Certificateless public key cryptography. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, 30 November–4 December 2003; Springer: Berlin/Heidelberg, Germany, 2003; pp. 452–473.
32. Yum, D.H.; Lee, P.J. Generic construction of certificateless signature. In Proceedings of the Australasian Conference on Information Security and Privacy, Sydney, Australia, 13–15 July 2004; Springer: Berlin/Heidelberg, Germany, 2004; pp. 200–211.
33. Li, X.X.; Chen, K.f.; Sun, L. Certificateless signature and proxy signature schemes from bilinear pairings. *Lith. Math. J.* **2005**, *45*, 76–83. [CrossRef]
34. Au, M.H.; Mu, Y.; Chen, J.; Wong, D.S.; Liu, J.K.; Yang, G. Malicious KGC attacks in certificateless cryptography. In Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security, Singapore, 20–22 March 2007; pp. 302–311.
35. He, D.; Chen, J.; Zhang, R. An efficient and provably-secure certificateless signature scheme without bilinear pairings. *Int. J. Commun. Syst.* **2012**, *25*, 1432–1442. [CrossRef]
36. Tsai, J.L.; Lo, N.W.; Wu, T.C. Weaknesses and improvements of an efficient certificateless signature scheme without using bilinear pairings. *Int. J. Commun. Syst.* **2014**, *27*, 1083–1090. [CrossRef]
37. Yeh, K.H.; Su, C.; Choo, K.K.R.; Chiu, W. A novel certificateless signature scheme for smart objects in the Internet-of-Things. *Sensors* **2017**, *17*, 1001. [CrossRef]
38. Jia, X.; He, D.; Liu, Q.; Choo, K.K.R. An efficient provably-secure certificateless signature scheme for Internet-of-Things deployment. *Ad Hoc Netw.* **2018**, *71*, 78–87. [CrossRef]
39. Yang, X.; Huang, X.; Liu, J.K. Efficient handover authentication with user anonymity and untraceability for mobile cloud computing. *Future Gener. Comput. Syst.* **2016**, *62*, 190–195. [CrossRef]
40. Sánchez-García, J.; García-Campos, J.M.; Reina, D.; Toral, S.; Barrero, F. On-siteDriverID: A secure authentication scheme based on Spanish eID cards for vehicular ad hoc networks. *Future Gener. Comput. Syst.* **2016**, *64*, 50–60. [CrossRef]
41. Ye, F.; Roy, S.; Wang, H. Efficient data dissemination in vehicular ad hoc networks. *IEEE J. Sel. Areas Commun.* **2012**, *30*, 769–779. [CrossRef]
42. Gamage, C.; Gras, B.; Crispo, B.; Tanenbaum, A.S. An identity-based ring signature scheme with enhanced privacy. In Proceedings of the 2006 Securecomm and Workshops, Baltimore, MD, USA, 28 August–1 September 2006; pp. 1–5.
43. Wang, T.; Tang, X. A more efficient conditional private preservation scheme in Vehicular Ad Hoc Networks. *Appl. Sci.* **2018**, *8*, 2546. [CrossRef]

44. Bayat, M.; Barmshoory, M.; Rahimi, M.; Aref, M.R. A secure authentication scheme for VANETs with batch verification. *Wirel. Netw.* **2015**, *21*, 1733–1743. [CrossRef]
45. Ming, Y.; Shen, X. PCPA: A practical certificateless conditional privacy preserving authentication scheme for vehicular ad hoc networks. *Sensors* **2018**, *18*, 1573. [CrossRef] [PubMed]
46. Cui, J.; Zhang, J.; Zhong, H.; Xu, Y. SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter. *IEEE Trans. Veh. Technol.* **2017**, *66*, 10283–10295. [CrossRef]
47. 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]
48. Saxena, N.; Choi, B.J.; Lu, R. Authentication and authorization scheme for various user roles and devices in smart grid. *IEEE Trans. Inf. Forensics Secur.* **2015**, *11*, 907–921. [CrossRef]
49. Evariste, T.; Kasakula, W.; Rwigema, J.; Datta, R. Optimal Exploitation of On-Street Parked Vehicles as Roadside Gateways for Social IoV—A Case of Kigali City. *J. Open Innov. Technol. Mark. Complex.* **2020**, *6*, 73. [CrossRef]
50. Ming, Y.; Cheng, H. Efficient certificateless conditional privacy-preserving authentication scheme in VANETs. *Mob. Inf. Syst.* **2019**, *2019*, 7593138. [CrossRef]
51. Kamil, I.A.; Ogundoyin, S.O. A big data anonymous batch verification scheme with conditional privacy preservation for power injection over vehicular network and 5G smart grid slice. *Sustain. Energy, Grids Networks* **2019**, *20*, 100260. [CrossRef]
52. Zhang, L.; Zhang, F.; Wu, Q.; Domingo-Ferrer, J. Simulatable certificateless two-party authenticated key agreement protocol. *Inf. Sci.* **2010**, *180*, 1020–1030. [CrossRef]
53. Bayat, M.; Pournaghi, M.; Rahimi, M.; Barmshoory, M. NERA: A new and efficient RSU based authentication scheme for VANETs. *Wirel. Netw.* **2019**, *26*, 1–16. [CrossRef]
54. Malhi, A.K.; Batra, S. An efficient certificateless aggregate signature scheme for vehicular ad-hoc networks. *Discret. Math. Theor. Comput. Sci.* **2015**, *17*, 317–338.
55. Xiong, H.; Guan, Z.; Chen, Z.; Li, F. An efficient certificateless aggregate signature with constant pairing computations. *Inf. Sci.* **2013**, *219*, 225–235. [CrossRef]