IETE Technical Review

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/titr20

A Comprehensive Survey on Certificateless Aggregate Signature in Vehicular Ad Hoc Networks

Eko Fajar Cahyadi & Min-Shiang Hwang

To cite this article: Eko Fajar Cahyadi & Min-Shiang Hwang (2022) A Comprehensive Survey on Certificateless Aggregate Signature in Vehicular Ad Hoc Networks, IETE Technical Review, 39:6, 1265-1276, DOI: 10.1080/02564602.2021.2017800

To link to this article: https://doi.org/10.1080/02564602.2021.2017800

Published online: 10 Jan 2022.

IETE TECHNICAL REVIEW
2022, VOL. 39, NO. 6, 1265–1276
https://doi.org/10.1080/02564602.2021.2017800

REVIEW ARTICLE

A Comprehensive Survey on Certificateless Aggregate Signature in Vehicular Ad Hoc Networks

Eko Fajar Cahyadi[1,2] and Min-Shiang Hwang[1,3]

[1]Department of Computer Science and Information Engineering, Asia University, Taichung 41354, Taiwan; [2]Faculty of Telecommunication and Electrical Engineering, Institut Teknologi Telkom Purwokerto, Purwokerto 53147, Indonesia; [3]Department of Medical Research, China Medical University Hospital, China Medical University, Taichung 40402, Taiwan

ABSTRACT

Research related to the authentication schemes in vehicular ad hoc networks (VANETs) has received significant attention recently. They substantially impact the security and privacy aspects of the message dissemination process in the road environment. Some authentication schemes with certificateless aggregate signature (CLAS) in VANETs have been published since the first related article emerged in 2015. This paper comprehensively reviews most of them regarding their main feature, contributions, security, and performance efficiency, as the state-of-the-art of all CLAS mechanisms in VANETs. Finally, the conclusion and some open issues on the CLAS authentication scheme in VANETs are provided in this survey.

KEYWORDS

Authentication Scheme; CLAS; Security; Survey; VANETs

1. INTRODUCTION

Vehicular ad hoc networks (VANETs) have the capability to provide information dissemination among the vehicles that will become the future of our road transportation systems. This approach aims to improve driving safety as its primary goal. VANETs are loaded with intelligent transportation system (ITS) properties, which will make all these smart vehicles communicate with each other via vehicle-to-vehicle (V2V) and the roadside unit (RSU) via vehicle-to-infrastructure (V2I) communications.

As shown in Figure 1, VANETs are made up of three primary components: the trusted authority (TA), the remote server unit (RSU), and the onboard unit (OBU). The trust and security management hub for all VANET entities is TA. Its responsibilities include RSU and OBU registration and parameter creation after they join the network. It also revokes nodes when vehicles send out fraudulent signals or hostile conduct [1–3]. Meanwhile, RSUs are fixed infrastructures entirely controlled by TA and are positioned along the road at specific areas such as intersections or parking lots. Their storage capacity is relatively limited compared to the TA. Therefore, they must transfer data to ITS's data centre regularly [4]. In addition, they provide a link between the TA and the vehicles (OBUs). RSUs are wired to the TA, while OBUs are connected through the dedicated short-range communications (DSRC) protocol [5].

Vehicles might broadcast a traffic-related message to hundreds of other vehicles (V2V) or RSUs (V2I) every 100–300 milliseconds in this new environment [5,6]. Every vehicle has an OBU that serves as a transceiver. It will broadcast information such as position, speed, and direction to improve the road environment, traffic safety, and vehicle mutual knowledge of local traffic conditions [3].

Despite the above benefits, security and privacy become key concerns due to their unique properties, such as open wireless communication, quick topology shift, high mobility, time-critical, and many messages interchange [7]. Signing each message with a digital signature is the most frequent method of guaranteeing the confidentiality of major message exchanges in VANETs. Meanwhile, an effective anonymous authentication strategy for VANETs must adhere to the VANETs' severe temporal constraints.

To satisfy the security and privacy requirements in VANETs, Lu *et al.* [2] distinguished the privacy-preserving authentication scheme of VANETs into five categories, including public key infrastructure (PKI)-based [6,8,9], symmetric cryptography based [10–12],

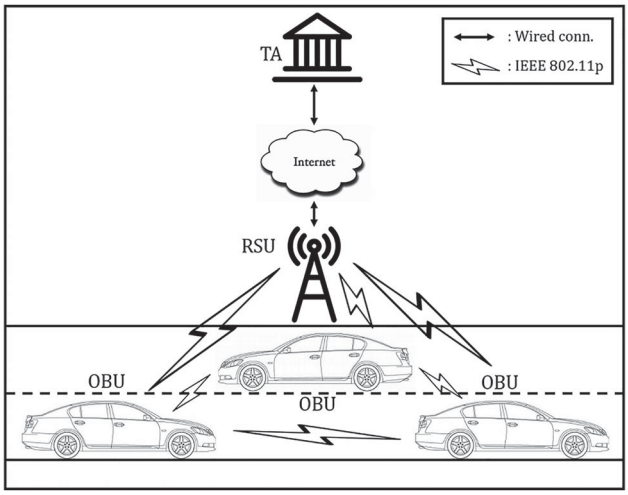

Figure 1: Topology of VANETs

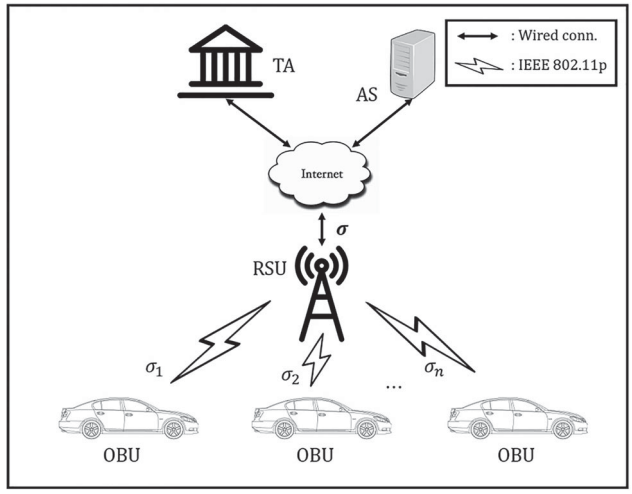

Figure 2: Aggregate signature in VANETs

identity (ID)-based signature [13–15], certificateless signature/certificateless aggregate signature (CLS/CLAS)-based [16–38], and group signature-based [3,39]. In traditional public-key cryptography (PKC), each public key is required to generate a corresponding digital certificate [40,41]. When Alice wants to send a message to Bob, firstly, she needs to obtain Bobs' identity, public key, and certificate. She then uses Bobs' public key to encrypt the message and sends it to him. This mechanism requires certification management that increases the verification time. In 1984, Shamir [42] proposed a new concept called ID-based public-key cryptography (ID-PKC) to solve the problems. The public key in ID-PKC consists of the users' identity information, such as phone number and email address. Therefore, it can solve the traditional PKC problem by generating no certificate [43]. However, the private key corresponding to the public key is generated by a key generating centre (KGC). If the KGC is compromised, the attacker will obtain all the private keys. Thus, attackers can arbitrarily decrypt other peoples' encrypted messages or forge signatures. This attack is called a key escrow problem.

To solve the key escrow problem, Al-Riyami-Paterson [44] were introduced certificateless public key cryptography (CL-PKC). In this scheme, the KGC generates part of the users' private key while the user generates the other part. As a result, the KGC no longer gets to know the users' entire private keys, and the key escrow problem is overcome [45]. Some scholars even extend the exploration with a certificateless signature (CLS) scheme in lattice-based cryptography [46,47]. However, another problem in VANETs is data compression. When RSUs send messages to the application server (AS), many signatures will be sent, putting a great strain on communication and storage. By using a scheme called aggregate signature, we can aggregate multiple signatures generated by different users for different messages into a single signature (see Figure 2). This approach not only reduces the length of the signature but also improves verification efficiency. Therefore, based on CL-PKC and aggregate signature's advantages, some scholars combined these two methods and proposed a certificateless aggregate signature (CLAS) mechanism. This mechanism effectively improves verifying a large number of messages in VANETs.

Keeping the aforesaid issue in mind, the CLAS method would be precious in resource-constrained scenarios such as VANETs since it may effectively cut computation and communication costs, notably in the signature verification time. Since its first appearance in 2015, at least 23 publications have covered CLAS authentication schemes in VANETs. However, to the best of our knowledge, there have been no survey articles published in recent years that completely cover this subject. As a result, this survey serves as the initial work for all existing CLAS schemes on VANETs, covering their primary features and contributions, cryptanalysis and improvements to other schemes, and comparing their security and performance.

For a better understanding, the rest of this survey is organised as follows. In Section 2, we provide preliminaries. Next, we introduce CLAS in VANET, and its system components and security model are introduced in Section 3. Section 4 presents the literature survey, including the main table related to the 23 CLAS schemes in VANETs publications carried out to the public, together with its security and performance comparisons. Finally,

we provide the conclusion and future challenges in Section 5.

2. PRELIMINARIES

This section discusses the topology of the CLAS scheme in VANETs, the concept of bilinear maps, complexity assumptions used to guarantee security in CLAS, and the basic security and privacy requirements in VANETs. Many survey papers generally examine the security and privacy in VANETs. This is because they both share the same VANETs' topology as the main object and the same CLAS mechanism as the common authentication scheme. Therefore, in this article, we mainly focused on their security and performance capabilities by these properties.

2.1 System Model

In general, VANETs' topology is composed of two layers. The upper layer comprises TA (*i.e.* KGC and tracking authorities (TRA)) and application server (AS). Meanwhile, the lower layer is filled by RSUs and OBUs [19,48–50]. KGC produces public system parameters and preloads them on RSUs and OBUs in the off-line/on-line mode. It also generates and distributes the partial private keys for RSUs and vehicles. On the other hand, TRA is responsible for registering RSU and vehicle, generating pseudonyms for the vehicle, and in case of dispute, it can trace the vehicle's real identity. In addition, AS is a traffic-related application server that serves safety-related applications. It will gather traffic-related messages sent by RSUs and do further traffic analysis [23,24]. In the CLAS-VANETs scheme, AS acts as the aggregate verifier of the aggregate signature from RSU. The topology of aggregate signature in VANETs is shown in Figure 2.

In this ecosystem, it is assumed [17,19,23,24]:

- The TRA and KGC are fully trusted and uncompromised. They are supported with enough power and storage capability.
- RSUs are semi-trusted (honest but curious). It has greater computation and power supports than OBU.
- Vehicles (OBUs) are equipped with a tamper-proof device (TPD) that is assumed to be credible. OBUs are not trusted. Therefore, every message that comes from the OBUs must be authenticated.

2.2 Characteristics of VANETs

As briefly mentioned in Section 1, VANETs have unique characteristics compared to the other wireless network environment [1,2].

- Open wireless communication: VANETs operates in the open wireless channel, which is naturally not secure. Therefore, the information that is disseminated between vehicles should be anonymous. So, anyone who has no access to the network, or intends to interrupt the message, cannot forge the messages and harmed the other users.
- Quick topology shift: Because of the significant mobility of vehicles, VANETs' topology is rapidly changed. As a result, VANETs are prone to attacks, and identifying rogue vehicles is challenging.
- High mobility: In reality, vehicles are move at high speed. Hence, connections between two nodes in VANETs usually only happen once and in a concise time. As a result, identifying the security of personal contacts in VANETs would be problematic.
- No power constraint: Since every vehicle has its battery, they get continuous power support and are not restricted by their energy usage.
- Computation and storage capability: The OBU device has relatively small capabilities of computation and storage. Therefore, to verify a large amount of information from the other vehicles, the network must be supported by adequate data compression and lightweight authentication schemes.
- Time-critical: The disseminated information in VANETs must be received by the other nodes in the particular time limit range. It is intended to allow the receiver to have enough time to make decisions and take appropriate measures.
- Variable network density: VANETs' network density is determined by vehicle traffic density, which can vary between rural and suburban regions, the intersections or highways, or during traffic jams and free time.

2.3 The Bilinear Maps

The bilinear map $\hat{e}$ can be obtained from the modified Weil pairing [51] or Tate pairing [52] on elliptic curves. Its security and complexity lie on the computational Diffie-Hellman problem (CDHP), which is believed to be difficult to solve [53]. Let G_1 be denoted as a cyclic additive group generated by P, and G_2 is a cyclic multiplicative group with the same prime order q. Let $\hat{e} : G_1 \times G_1 \rightarrow G_2$ be a bilinear map if it satisfies the following properties:

- Bilinear: For all $P, Q, R \in G_1$, we have $\hat{e}(Q, P + R) = \hat{e}(P, Q + R) = \hat{e}(Q, P) \cdot \hat{e}(Q, R)$. For any $a, b \in Z_q^*$, $\hat{e}(aQ, bP) = \hat{e}(bQ, aP) = \hat{e}(Q, P)^{ab}$.

- Computable: For any $P, Q \in G_1$, there is an efficient algorithm to compute $\hat{e}(P, Q)$.
- Non-degenerate: $\hat{e}(P, Q) \neq 1$.

2.4 Elliptic Curve Cryptography (ECC)

The elliptic curve cryptography (ECC), commonly used in cryptography, is an outstanding algorithm with incredibly high efficiency and relatively good security. Miller [54] and Koblitz [55] designed it for resource-constrained environments that offer equivalent security to RSA with far smaller key size. It requires less storage and hence reduces the processing overhead [37]. If F_q is a field and E_p is an elliptic curve, then $E_p(F_q)$ is a group. For $E_p(F_q)$, we read it elliptic curve E_p over field F_q, which indicates the set of points on E_p along with only a single addition operation defined for $E_p(F_q)$ [56]. Therefore, it is impossible to multiply or divide elements of $E_p(F_q)$. The scalar multiplication algorithm kP is the most basic and time-consuming operation in the ECC, where k is an integer, P is a point defined on the elliptic curve E_p on the field F_q, and $kP = P + P + \cdots + P$. It determines the ECC's operation speed [57]. The elliptic curve discrete logarithm problem (ECDLP) complexity assumption built on ECC is discussed in the subsequent section.

2.5 Complexity Assumptions

In general, there are two main hard problems and assumptions that are widely used in any authentication scheme that are built on the bilinear maps and ECC, respectively. We describe them as follows.

2.5.1 Computational Diffie-Hellman Problem (CDHP)

In CDHP, G_1 is a cyclic additive group generated by P (see Section 2.3.), with given $P, aP, bP \in G_1$, and $a, b \in Z_q^*$ are unknown values. The CDHP is difficult to solve by adversary $\mathcal{A}$, because there is no polynomial time algorithm that can discover $abP \in G_1$.

2.5.2 Elliptic Curve Discrete Logarithm Problem (ECDLP)

Let F_p be a finite field determined by a prime number p. Meanwhile, E_p is elliptic curve points over F_p, defined by: $y^2 = x^3 + \alpha x + \beta \mathrm{mod} p$, where $\alpha, \beta \in F_p$ and $(4\alpha^3 + 27\beta^2) \mathrm{mod} p \neq 0$. The additive group G of the elliptic curve includes points over E_p/F_p and O, where O is point at infinity. G forms a cyclic group under addition operations $R = P + Q$, for $P, Q \in G$ by the chord-and-tangent rule [50,54,55]. Suppose P is a generator of G in order of q, we define the scalar multiplication as, $kP = P + P + \cdots + P$ (k times), with $k \in Z_q^*$. By given two random point $P, Q \in G$ on E_p, where $Q = xP$, it is difficult to calculate $x \in Z_q^*$ from Q.

2.6 Security and Privacy Requirements

As depicted in Figure 2, the V2 V and V2I communications are established under an open wireless communication channel, so it is vulnerable to various attacks. To design a secure authentication mechanism, we define the security and privacy requirements that need to be met in VANET [44,48,58,59].

- **(S1)** Non-repudiation: Messages' sender cannot deny the information they have sent.
- **(S2)** Identity Privacy-preserving: The identity of the messages' sender should be anonymous, and only TA can reveal their real identity.
- **(S3)** Message Authentication: The receiver must be capable of differentiating the original message from the bogus message.
- **(S4)** Traceability: TA must be able to reveal the real identities of the users' pseudoidentities in the case of a dispute.
- **(S5)** Replaying Attack Resistance: The networks could endure a passive data capture and subsequent retransmission to produce an unauthorised message by the adversaries.
- **(S6)** Unlinkability: An adversary (vehicle or RSU) should not link two or more subsequent pseudonym messages of the same vehicle.
- **(S7)** Impersonation Attack Resistance: The networks could endure towards the attacker trying to assume or impersonate the identity of the legitimate vehicles in VANETs, to generate the signature for any messages.

3. CLAS IN VANETS

This section discusses the main concept of the CLAS mechanism and the publication list that covers the CLAS authentication scheme in VANETs [16–38].

3.1 System Components

Generally, a CLAS-VANETs scheme includes eight following algorithms (see Figure 3): *Setup*, *PseudonymGen*, *PartialPrivateKeyGen*, *VehicleKeyGen*, *Sign*, *Verify*, *Aggregate*, and *AggregateVerify*.

- *Setup* ($1^l \rightarrow P_{pub}, s, params$): TRA and KGC run this algorithm with a security parameter $l \in Z_q^*$ as input to produces master public key P_{pub}, master secret key s, and public parameters *params*.

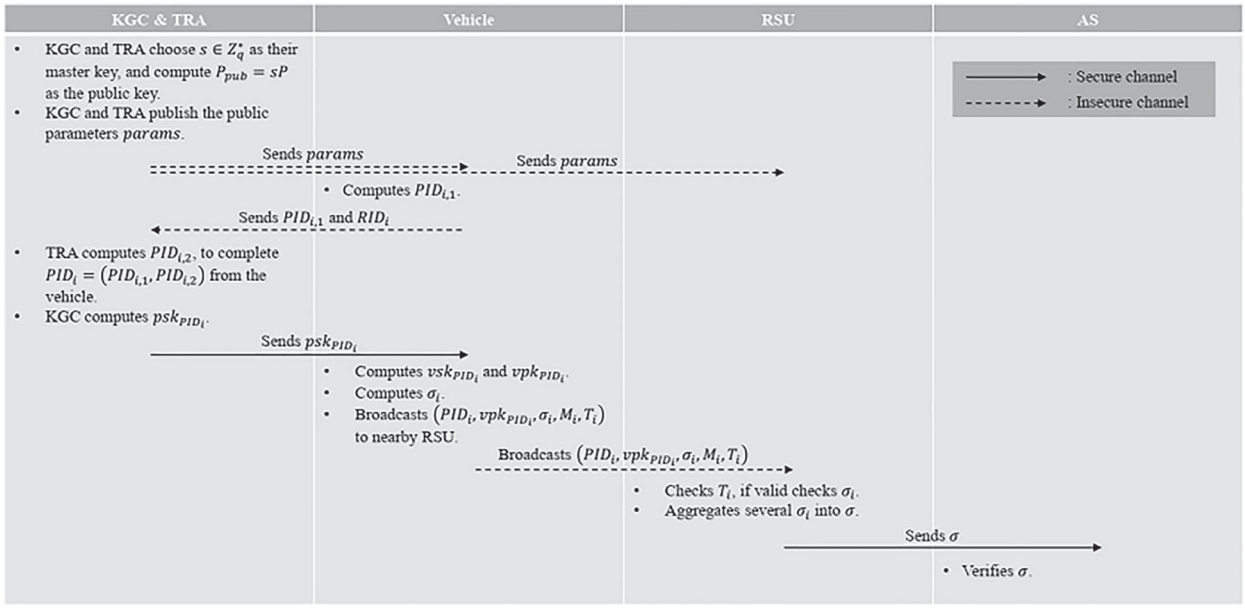

Figure 3: General CLAS scheme procedures in VANETs

- *PseudonymGen*: TRA run this algorithm by inputs vehicle's real identity RID_i and outputs vehicle's pseudo-identity PID_i.
- *PartialPrivateKeyGen*: KGC inputs PID_i and *params* to produce respective partial private key psk_{PID_i}.
- *VehicleKeyGen*: Vehicle takes *params* and its psk_{PID_i} to generates its private and public keys vsk_{PID_i} and vpk_{PID_i}, respectively.
- *Sign*: Vehicle inputs *params* together with its PID_i, psk_{PID_i}, vsk_{PID_i}, and the message M_i. It returns the signature σ_i on M_i. Together with a timestamp T_i, vehicle sends $\sigma_i, M_i, PID_i, vpk_{PID_i}, T_i$ to RSU.
- *Verify*: As the verifier, RSU takes $\sigma_i, M_i, PID_i, vpk_{PID_i}$ as the input. If σ_i is valid, the RSU accepts it, otherwise rejects.
- *Aggregate*: After σ_i is accepted, as the aggregator, RSU inputs n vehicles' signatures $(\sigma_1, \sigma_2, \cdots, \sigma_n)$ on n distinct messages $(M_1, M_2, \cdots, M_n)$. Then, the outputs the aggregate signature σ on $(M_1, M_2, \cdots, M_n)$. The aggregator sends σ to the aggregate verifier.
- *AggregateVerify*: As the aggregate verifier, the application server (AS) inputs n vehicles' public keys $(vpk_{PID_1}, vpk_{PID_2}, \cdots, vpk_{PID_n})$, the vehicles' pseudonyms $(PID_1, PID_2, \cdots, PID_n)$, and the corresponding aggregate signature σ on the message set $(M_1, M_2, \cdots, M_n)$. Finally, if this signature is valid, the aggregate verifier accepts it, otherwise rejects.

3.2 Security Model

After considering various security parameters described as (S1)–(S7), depending on the behaviour of adversary $\mathcal{A}$, we consider the two types of adversaries called Type-1 adversary ($\mathcal{A}_1$) and Type-2 adversary ($\mathcal{A}_2$).

3.2.1 Type-1 Adversary ($\mathcal{A}_1$)

The $\mathcal{A}_1$ can compromises or replace a users' public key with any value but cannot access KGCs' master secret key.

3.2.2 Type-2 Adversary ($\mathcal{A}_2$)

The $\mathcal{A}_2$ can access the KGCs' master key but cannot replace the users' public key.

A CLAS scheme is said to be existentially unforgeable against adaptive chosen message and identity attacks by considering the following two games, Game-1 and Game-2, against $\mathcal{A} \in \{\mathcal{A}_1, \mathcal{A}_2\}$. Both $\mathcal{A}_1$ and $\mathcal{A}_2$ can access the following five oracles:

- *CreateUser*: After receiving a PID_i this oracle returns vpk_{PID_i} to $\mathcal{A}$.
- *RevealPartialPrivateKey*: After receiving a vehicles' PID_i, the corresponding psk_{PID_i} is returned to $\mathcal{A}$ by this oracle.
- *RevealPrivateKey*: After receiving a vehicles' PID_i, the corresponding vsk_{PID_i} is returned to $\mathcal{A}$ by this oracle.
- *ReplaceKey*: After receiving a new public key $vpk_{PID_i}^*$ chosen by $\mathcal{A}$ and a PID_i, this oracle updates vehicles' vpk_{PID_i} with $vpk_{PID_i}^*$.
- *Sign*: After receiving Wednesday, January 5, 2022 at 8:25 am PID_i and $M_i \in \{(0,1)^*\}$, a σ_i of M_i is returned to $\mathcal{A}$ by this oracle.

3.2.3 Game-1

The challenger $\mathcal{C}$ deals with $\mathcal{A}_1$ executes the following steps.

- *Setup*: $\mathcal{C}$ runs Setup algorithm, which takes l to generate s and *params*. The params is sent by $\mathcal{C}$ to $\mathcal{A}_1$ while keeps s as secret to itself.
- *Query*: The $\mathcal{A}_1$ is allowed to run *CreateUser*, *RevealPartialPrivateKey*, *RevealPrivateKey*, and *Sign* oracles.
- *Forgery*: Finally, $\mathcal{A}_1$ outputs an aggregate signature σ_n^* on the messages set $(M_1^*, M_2^*, \cdots, M_n^*)$ corresponding to targeted identities $(PID_1^*, PID_2^*, \cdots, PID_n^*)$ with public keys $(vpk_{PID_1^*}, vpk_{PID_2^*}, \cdots, vpk_{PID_n^*})$.

Table 1: Literature survey of CLAS schemes in VANETs

Author & Year	Literature	Main feature and contributions
Malhi-Batra [16]–(2015)	An efficient certificateless aggregate signature scheme for vehicular ad hoc networks.	The scheme comprises nine algorithms: *Setup*, *Registration*, *PartialPrivateKeyGen*, *VehicleKeyGen*, *PseudonymGen*, *Sign*, *Verify*, *Aggregate*, and *AggregateVerify*. Together with [17], they become the first two CLAS schemes in VANETs with partial aggregation.
Horng *et al.* [17]–(2015)	An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks.	The scheme comprises seven algorithms: *Setup*, *PseudonymGen* / *PartialPrivateKeyGen*, *VehicleKeyGen*, *Sign*, *Verify*, *Aggregate*, and *AggregateVerify*. Partial aggregation CLAS scheme that claimed more efficient than the other CLAS scheme [42]. The RSU as the verifier also does batch verification.
Li *et al.* [18]–(2016)	Cryptanalysis and improvement of certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks.	The scheme comprises seven algorithms: *Setup*, *PseudonymGen* / *PartialPrivateKeyGen*, *VehicleKeyGen*, *Sign*, *Verify*, *Aggregate*, and *AggregateVerify*. Partial aggregation CLAS scheme. Make cryptanalysis and improvement to [17]. Li *et al.* shows if Horng *et al.*'s scheme is vulnerable to malicious-but-passive KGC attacks.
Cui *et al.* [19]–(2018)	An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks.	The scheme comprises seven algorithms: *Setup*, *PseudonymGen* / *PartialPrivateKeyGen*, *VehicleKeyGen*, *Sign*, *Verify*, *Aggregate*, and *AggregateVerify*. Partial aggregation CLAS scheme that claimed more efficient than [17,42]. The RSU as the verifier also does batch verification.
Kumar-Sharma [20]–(2018)	On the security of certificateless aggregate signature scheme in vehicular ad hoc networks.	The scheme comprises seven algorithms: *Setup*, *PartialPrivateKeyGen*, *VehicleKeyGen*, *PseudonymGen*, *Sign*, *Verify*, and *AggregateVerify*. Partial aggregation CLAS scheme. Make a cryptanalysis and improvement to [19]. Kumar-Sharma shows if Cui *et al.*'s scheme is insecure against Type-2 adversary attack.
Yang *et al.* [21]–(2018)	An improved certificateless aggregate signature scheme for vehicular ad-hoc networks.	The scheme comprises eight algorithms: *Setup*, *PartialPrivateKeyGen*, *VehicleKeyGen*, *PseudonymGen*, *Sign*, *Verify*, *Aggregate*, and *AggregateVerify*. Partial aggregation CLAS scheme. Make a cryptanalysis and improvement to [20]. Yang *et al.* shows if Kumar-Sharma's scheme is insecure against attacks from internal signers and coalition attacks from a malicious KGC and RSU. However, Yang *et al.*'s scheme has a higher computational cost in the *AggregateVerify* compared to Kumar-Sharma's.
Kumar *et al.* [22]–(2019)	Secure CLS and CLAS schemes designed for VANETs.	The scheme comprises nine algorithms: *Setup*, *Registration*, *PartialPrivateKeyGen*, *VehicleKeyGen*, *PseudonymGen*, *Sign*, *Verify*, *Aggregate*, and *AggregateVerify*. This is a partial aggregation CLAS scheme.
Zhong *et al.* [23]–(2019)	Privacy-preserving authentication scheme with full aggregation in VANET.	The scheme comprises eight algorithms: *Setup*, *PseudonymGen*, *PartialPrivateKeyGen*, *VehicleKeyGen*, *Sign*, *Verify*, *Aggregate*, and *AggregateVerify*. This is a full aggregation CLAS scheme that claimed more efficient than [16].
Kamil-Ogundoyin [24]–(2019)	An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks.	The scheme comprises nine algorithms: *Setup*, *Registration*, *PartialPrivateKeyGen*, *PseudonymGen*, *VehicleKeyGen*, *Sign*, *Verify*, *Aggregate*, and *AggregateVerify*. This is a full aggregation CLAS scheme that more efficient than [16–19,22]. The authors make a cryptanalysis and improvement to Cui *et al.*'s scheme, and show if the scheme is vulnerable against forgery attacks in Type-2 adversary. The RSU as the verifier also does batch verification.
Zhao *et al.* [25]–(2019)	An efficient certificateless aggregate signature scheme for the internet of vehicles.	The scheme comprises nine algorithms: *Setup*, *Registration*, *PseudonymGen*, *PartialPrivateKeyGen*, *VehicleKeyGen*, *Sign*, *Verify*, *Aggregate*, and *AggregateVerify*. This is a partial aggregation CLAS scheme that more efficient than [17,19,22,24,28]. The authors make cryptanalysis and improvement towards Hu *et al.*'s scheme, and show if the scheme cannot withstand forgery attacks.
Hu *et al.* [26]–(2019)	Security analysis of certificateless aggregate signature scheme in VANETs.	The scheme comprises nine algorithms: *Setup*, *Registration*, *PartialPrivateKeyGen*, *VehicleKeyGen*, *PseudonymGen*, *Sign*, *Verify*, *Aggregate*, and *AggregateVerify*. This is a partial aggregation CLAS scheme that makes cryptanalysis and improvement to [60] shows if the scheme cannot withstand forgery attacks.
Zhao-Zhang [27]–(2019)	Privacy-protected certificateless aggregate signature scheme in VANET.	The scheme comprises seven algorithms: *Setup*, *Registration*, *VehicleKeyGen*, *Sign*, *Aggregate*, *Verify*, and *AggregateVerify*. This is a partial aggregation CLAS scheme.
Ali *et al.* [28]–(2019)	A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs.	The scheme comprises eight algorithms: *Setup*, *PseudonymGen*, *PartialPrivateKeyGen*, *VehicleKeyGen*, *Sign*, *Verify*, *Aggregate*, and *AggregateVerify*. In addition, the authors include blockchain to implement pseudo-identities revocation transparency before verifying the signatures. It is also more efficient in the *Verify* and *AggregateVerify* processes than the other CLAS schemes in VANETs [16–18,22]. The RSU as the verifier also does batch verification.

(*continued*).

Table 1: Continued.

Author & Year	Literature	Main feature and contributions
Li *et al.* [29]–(2019)	An efficient conditional privacy-preserving authentication scheme for vehicular ad hoc networks using online/offline certificateless aggregate signature.	The scheme comprises eight algorithms: *Setup*, *PseudonymGen*, *PartialPrivateKeyGen*, *OfflineSign*, *OnlineSign*, *Verify*, *Aggregate*, and *AggregateVerify*. The authors proposed an online/offline signature to further decrease the computation cost. The heavy computations are executed in the offline phase, resulting in the intermediate output that will be executed later in the online phase. Since the scheme is pairing-free, it is more efficient than several pairing-based CLAS schemes in VANETs [16,17,23]. The RSU as the verifier also does batch verification.
Li *et al.* [30]–(2020)	An efficient certificateless aggregate signature scheme designed for VANET.	The scheme comprises eight algorithms: Setup, PseudonymGen, PartialPrivateKeyGen, VehicleKeyGen, Sign, Verify, Aggregate, and AggregateVerify. This scheme is more efficient than [20,22–24,60] The authors make cryptanalysis and improvement to Zhong *et al.*'s scheme and show if the scheme is vulnerable against forgery attack in Type- 2 adversary
Xu *et al*. [31]–(2020)	Efficient certificateless aggregate signature scheme for performing secure routing in VANETs.	The scheme comprises seven algorithms: *Setup*, *PartialPrivateKeyGen*, *VehicleKeyGen*, *Sign*, *Verify*, *Aggregate*, and *AggregateVerify*. This is a partial aggregation CLAS scheme.
Kamil-Ogundoyin [32]–(2020)	On the security of privacy-preserving authentication scheme with full aggregation in vehicular ad hoc network.	The scheme comprises eight algorithms: *Setup*, *PseudonymGen*, *PartialPrivateKeyGen*, *VehicleKeyGen*, *Sign*, *Verify*, *Aggregate*, and *AggregateVerify*. This is a full aggregate CLAS scheme that makes cryptanalysis and improvement to [23]. The authors show if Zhong *et al.*'s scheme is vulnerable against signature forgery attacks by a Type-2 adversary.
Hu *et al.* [33]–(2020)	Certificateless aggregate signature scheme with high efficiency in vehicular ad-hoc network.	The scheme comprises nine algorithms: *Setup*, *Registration*, *VehicleKeyGen*, *PartialPrivateKeyGen*, *PseudonymGen*, *Sign*, *Verify*, *Aggregate*, and *AggregateVerify*. This partial aggregation CLAS scheme is an improvement of [60].
Mei *et al.* [34]–(2021)	Efficient certificateless aggregate signature with conditional privacy preservation in IoV.	The scheme comprises eight algorithms: *Setup*, *PseudonymGen*, *PartialPrivateKeyGen*, *VehicleKeyGen*, *Sign*, *Verify*, *Aggregate*, and *AggregateVerify*. This full aggregate CLAS scheme is more efficient than [20–22].
Thumbur *et al.* [35]–(2021)	Efficient and secure certificateless aggregate signature-based authentication scheme for vehicular ad hoc networks.	The scheme comprises nine algorithms: *Setup*, *PseudonymGen*, *PartialPrivateKeyGen*, *SetSecretValue*, *VehicleKeyGen*, *Sign*, *Verify*, *Aggregate*, and *AggregateVerify*. Compared to the other CLAS schemes in VANETs that employ CDHP complexity assumption, this scheme results in apparent advantages in efficiency.
Vallent *et al.* [36]–(2021)	Efficient certificate-less aggregate signature scheme with conditional privacy-preservation for vehicular ad hoc networks enhanced smart grid system.	The scheme comprises eight algorithms: *Setup*, *PseudonymGen*, *PartialPrivateKeyGen*, *VehicleKeyGen*, *Sign*, *Verify*, *Aggregate*, and *AggregateVerify*. It is considered applicable to improve the current traditional electricity grid for future electric vehicle charging. However, there is no further technical discussion related to smart grid application in this paper. This scheme is more efficient in the *Sign*, *Verify*, and *AggregateVerify* phases than [17,19,27].
Ye *et al.* [37] – (2021)	Certificateless-based anonymous authentication and aggregate signature scheme for vehicular ad hoc networks.	The scheme comprises seven algorithms: *Setup*, *PartialPrivateKeyGen*, *VehicleKeyGen*, *Sign*, *Verify*, *Aggregate*, and *AggregateVerify*. The authors made cryptanalysis towards [24] and revealed its weakness to coalition attacks from malicious vehicles. In addition, this scheme is more efficient in the *Sign*, *Verify*, and *AggregateVerify* phases than [16,21,22,25].
Ren *et al.* [38]–(2021)	Privacy-preserving batch verification signature scheme based on blockchain for vehicular ad-hoc networks.	The scheme comprises eight algorithms: *Setup*, *PartialPrivateKeyGen*, *VehicleKeyGen*, *PseudonymGen, Sign*, *Verify*, *Aggregate*, and *AggregateVerify*. The scheme utilises blockchain to verify the legality of the vehicle's identity and performs batch verification in the *Verify* phase. It is more efficient in the *Sign*, *Verify*, and *AggregateVerify* phase than [16,17,22]. The RSU as the verifier also does batch verification.

In this case, $\mathcal{A}_1$ wins Game-1 if:

- The σ_n^* is a valid aggregate signature on $(M_1^*, M_2^*, \cdots, M_n^*)$ with identities $(PID_1^*, PID_2^*, \cdots, PID_n^*)$ and public keys $(vpk_{PID_1^*}, vpk_{PID_2^*}, \cdots, vpk_{PID_n^*})$.
- The PID_i^* has not queried partial private key $psk_{PID_i^*}$ during *RevealPartialPrivateKey* queries.
- *Sign* oracle has never been queried with PID_i^* and M_i^*.

Definition 1: If $\mathcal{A}_1$ cannot win Game-1 with non-negligible advantage in polynomial time, the CLAS scheme is secure against $\mathcal{A}_1$.

3.2.4 Game-2

The challenger $\mathcal{C}$ deals with $\mathcal{A}_2$ executes the following steps.

- *Setup*: $\mathcal{C}$ runs *Setup* algorithm, which takes l to generate s and *params*. Both s and *params* are sent by $\mathcal{C}$ to $\mathcal{A}_2$.
- Query: *The* $\mathcal{A}_2$ *is allowed to run* CreateUser, RevealPrivateKey, ReplaceKey, *and* Sign *oracles. The* $\mathcal{A}_2$ *is no longer needs* RevealPartialPrivateKey *since it has the access to* s.

- *Forgery*: Finally, $\mathcal{A}_2$ outputs an aggregate signature σ_n^* on the messages set $(M_1^*, M_2^*, \cdots, M_n^*)$ corresponding to targeted identities $(PID_1^*, PID_2^*, \cdots, PID_n^*)$ with public keys $(vpk_{PID_1^*}, vpk_{PID_2^*}, \cdots, vpk_{PID_n^*})$.

In this case, $\mathcal{A}_2$ wins Game-2 if:

- The σ_n^* is a valid aggregate signature on $(M_1^*, M_2^*, \cdots, M_n^*)$ with identities $(PID_1^*, PID_2^*, \cdots, PID_n^*)$ and public keys $(vpk_{PID_1^*}, vpk_{PID_2^*}, \cdots, vpk_{PID_n^*})$.
- The PID_i^* has not queried private key $vsk_{PID_i^*}$ during *RevealPrivateKey* queries.
- *Sign* oracle has never been queried with PID_i^* and M_i^*.

Definition 2: If $\mathcal{A}_2$ cannot win Game-2 with non-negligible advantage in polynomial time, the CLAS scheme is secure against $\mathcal{A}_2$.

From the **Definition 1** and **Definition 2** above, a CLAS scheme is claimed to be existentially unforgeable under an adaptive chosen message attack, if there exists no polynomial-time adversary $\mathcal{A}_1$ and $\mathcal{A}_2$ with a non-negligible advantage in Game-1 and Game-2, respectively.

4. LITERATURE ANALYSIS

This section deals with the literature analysis, including the security and performance comparisons of several CLAS schemes in VANETs [16–38]. We present the literature survey in Table 1, specifically express the number of algorithms used by the authors, their cryptanalysis towards the other scheme, and their security and performance compared to other methods, as their main features and contribution. The number of the implemented algorithms is based on the general CLAS scheme discussion in Section 3.1, by keeping each references' original notion. For example, since the authors in [17–19] described their scheme constructed of seven algorithms, so we keep count it as seven instead of eight, although *PseudonymGen* and *PartialPrivateKeyGen* can be separated as two different algorithms. Meanwhile, schemes that come without the *Registration* algorithm in it, some of them have included that process in *PseudonymGen*.

4.1 Security Comparison

Combining traffic data from vehicles in the vehicular network for further processing and exchange is critical. The security of traffic data aggregation should be assured since incorrect traffic data feedback can compromise traffic safety [60]. As previously discussed in Section 3.2., in the security model, we have two types of adversaries, $\mathcal{A}_1$ and $\mathcal{A}_2$. We can have security games by them, where $\mathcal{A}$ can interact with $\mathcal{C}$ to do some queries in the oracles. A formal security proof on the corresponding security game must be used to declare that a cryptographic method is secure [61].

Table 2: Security comparison

Ref.	S.$\mathcal{A}_1$	S.$\mathcal{A}_2$	S1	S2	S3	S4	S5	S6	S7
[16]	V	X [20]	V	X [62]	X [63]	V	X [63]	V	X [63]
[17]	X [25]	X [18]	V	V	X [63]	V	X [63]	V	X [63]
[18]	X [25*]	V	V	V	X [63*]	V	X [63*]	V	X [63*]
[19]	V	X [24,25,30]	V	V	V	V	V	V	V
[20]	V	X [21,34]	V	V	V	V	X [34]	X [34]	V
[21]	V	V	V	V	V	X [34]	X [34]	X [34]	V
[22]	X [30]	X [34]	V	V	V	V	V	V	V
[23]	V	X [30,32,34]	V	V	V	V	V	V	V
[24]	X [25]	X [25]	V	V	V	V	V	V	V
[25]	V	V	V	V	V	V	V	V	V
[26]	V	V	V	V	V	V	V	V	V
[27]	V	V	V	V	V	V	V	V	V
[28]	V	V	V	V	V	V	V	V	V
[29]	V	V	V	V	V	V	V	V	V
[30]	V	V	V	V	V	V	V	V	V
[31]	V	V	V	V	V	V	V	V	V
[32]	V	V	V	V	V	V	V	V	V
[33]	V	V	V	V	V	V	V	V	V
[34]	V	V	V	V	V	V	V	V	V
[35]	V	V	V	V	V	V	V	V	V
[36]	V	V	V	V	V	V	V	V	V
[37]	V	V	V	V	V	V	V	V	V
[38]	V	V	V	V	V	V	V	V	V

*Cryptanalysis to [18] that related to [17].
V: Satisfied.
X: Not satisfied.

Every author undoubtedly considers their scheme to be secure and capable against the most known attacks described in Section 2.6. and Section 3.2. However, there is also always someone who does cryptanalysis work towards those schemes. Therefore, we compare the security requirements in Table 2, indicating certain attacks can occur in the particular scheme. The other authors reveal these weaknesses by doing a detailed cryptanalysis work or just a simple comparison against two games with $\mathcal{A}_1$ and $\mathcal{A}_2$, and all security requirements (S1–S7).

In Table 2, the asterisk ($_*$) in [18] shows if the scheme does not withstand S.$\mathcal{A}_1$, S3, S5, and S7, just like [17]. This happens because [18] just made a minor modification towards [17] and left most of the phases unmodified. Therefore, circumstantially [25] and [64] also make the same cryptanalysis to [18]. Furthermore, we can see from Table 2 that references [25–38] still have no cryptanalysis from other publications since they are considerably new.

4.2 Performance Comparison

The performance comparisons presented in Table 3 are primarily related to *Sign* cost, *Verify* cost, and

Table 3: Performance comparison

Ref.	Hard problem	Sign	Verify	AggregateVerify
[16]	CDHP	$3SC$	$3PC + 3SC$	$3PC + 3nSC$
[17]	CDHP	$2SC$	$3PC + SC + HC$	$3PC + nSC + nHC$
[18]	CDHP	$2S$	$3PC + SC + HC$	$3PC + nSC + nHC$
[19]	ECDLP	S_EC	$3S_EC$	$(n+2)S_EC$
[20]	CDHP	$3SC$	$3PC + 3SC$	$3PC + 3nSC$
[21]	CDHP	$3SC$	$3PC + 3SC$	$3PC + 3nSC$
[22]	CDHP	$3SC$	$3PC + 3SC$	$3PC + 3nSC$
[23]	CDHP	$3SC$	$3PC + 2SC + HC$	$3PC + 2nSC + nHC$
[24]	ECDLP	$3S_EC$	$2S_EC$	$2S_EC$
[25]	ECDLP	S_EC	$4S_EC$	$(n+2)S_EC$
[26]	CDHP	$3SC$	$3PC + 3SC$	$3PC + 3nSC$
[27]	CDHP	$5SC$	$4PC + 2SC$	$4PC + 7nSC$
[28]	CDHP	SC	$PC + SC$	$PC + nSC$
[29]	ECDLP	S_EC	$3S_EC$	$(n+2)S_EC$
[30]	ECDLP	S_EC	$3S_EC$	$(n+2)S_EC$
[31]	CDHP	$3SC + HC$	$3PC + 2SC + 2HC$	$3PC + 2nSC + (n+1)HC$
[32]	CDHP	$3SC$	$3PC + 2SC + HC$	$3PC + 2nSC + nHC$
[33]	CDHP	$3SC$	$2PC + 3SC$	$2PC + 3nSC$
[34]	CDHP	$4SC + 2HC$	$4PC + 2SC$	$4PC + 2nSC$
[35]	ECDLP	S_EC	$3S_EC$	$(2n+1)S_EC$
[36]	ECDLP	S_EC	$2S_EC$	$2nS_EC$
[37]	ECDLP	S_EC	$2S_EC$	$(n+1)S_EC$
[38]	CDHP	$2SC$	$2PC$	$2PC$

AggregateVerify cost. The main goal is to reduce sign verification cost so that the signature verification process in V2I and V2 V could be done faster. We also present the complexity assumptions (hard problem) used in every scheme, based on the description in Section 2.5. All researchers used a pairing scheme (CDHP) or a pairing-free CLAS scheme (ECDLP). The CDHP operation is indeed generating more cost compared to ECDLP since they are utilising a bilinear pairing. Let PC denote the time of a pairing operation cost, SC is the time of a scalar multiplication cost in bilinear operation G_1, HC is the time of a MapToPoint hash operation cost, S_EC is a scalar multiplication cost in ECC operation, and n in *AggregateVerify* cost is the number of the verified messages. In CDHP, PC is the most time-consuming one compared to SC and HC. We only consider these four operations regarding their significance.

So far, there are two main approaches used by several authors to compute the computation cost in CLAS-VANETs subject. Some lead experiments setup [13,17,22,23,50] observes the processing time for the Tate pairing on a 159-bit subgroup of an MNT curve with an embeds degree 6 at an 80-bit security level and running on an Intel i7 3.07 GHz CPU. The obtained results for PC, SC, and HC are 3.21 , 0.39 , and 0.09 ms, respectively. Meanwhile, in another works [19,24,30] that intend to provide an equivalent security level to both CDHP and ECDLP-based complexity, the bilinear pairing $\hat{e} : G_1 \times G_1 \rightarrow G_2$ on the security level of 80 bits is created on a super singular elliptic curve E_p/F_p : $y^2 = x^3 + x \bmod p$ with embeds degree 2, with p consisting of a 512-bit prime number and q in $\hat{e}$ consisting of a 160-bit Solinas [65] prime number. The ECC is constructed as G is an additive group generated by a point P on a non-singular elliptic curve $E_p/F_p : y^2 = x^3 + ax + \beta \bmod p$, and its order is q, where (p, q) are two 160-bit prime numbers and $a, b \in Z_q^*$. In the latter experiments, resulting PC, SC, HC, and S_EC for 4.2110, 1.7090, 4.406, and 0.4420 ms, respectively. From the two approaches discussed above, we can refer the Table 3 in both ways.

5. CONCLUSION AND FUTURE RESEARCHES

Cryptographic schemes play a central role to ensures the security and privacy of any authentication protocols. In the CLAS authentication scheme, VANETs can experiences an improvement of signature verification time due to batch verification, signature aggregation, and aggregate verification processes in RSU and AS, respectively. This survey has comprehensively discussed the topology CLAS mechanisms in VANETs and detailed the number of their implemented algorithms, their cryptanalysis-improvement to other schemes, and their security efficiency as the main contribution. The main goal of this paper is to give state-of-the-art research in CLAS mechanism in VANETs so that any researchers who are relatively new to this area can benefit from the current research works in a promising way.

Due to the significant mobility of vehicles, rapid topology conversion remains a challenge. In addition, VANET is vulnerable to attacks, and it is challenging to identify rogue vehicles. In addition, there are still some works to be done in future research, such as the inefficiency caused by illegal/malicious messages in the *AggregateVerify* phase. However, with some modifications, the CLAS authentication scheme can be improved to identify this type of illegal information while retaining the rest of the legal information that is usually verified.

Another future research is the quantitative analysis of certificateless aggregate signatures in VANET, such as the number of publications per year, the number of each publisher, and the comparison of the number of journals and publications.

ACKNOWLEDGEMENT

The Ministry of Science and Technology partially supported this research, Taiwan (R.O.C.), under contract no.: MOST 109-2221-E-468-011-MY3 and MOST 110-2622-8-468-001-TM1.

FUNDING

This research was partially supported by the Ministry of Science and Technology, Taiwan (ROC), under contract no.: MOST 109-2221-E-468-011-MY3 & MOST 110-2622-8-468-001 -TM1.

REFERENCES

1. M. Azees, P. Vijayakumar, and L. J. Deborah, "Comprehensive survey on security services in vehicular ad-hoc networks," *IET Intel. Transport Syst.*, Vol. 10, no. 6, pp. 379–88, 2016. doi:10.1049/iet-its.2015.0072

2. Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, Vol. 20, no. 2, pp. 760–76, 2019. doi:10.1109/TITS.2018.2818888

3. X. Zhu, S. Jiang, L. Wang, and H. Li, "Efficient privacy-preserving authentication for vehicular ad hoc network," *IEEE Trans. Veh. Tech.*, Vol. 63, no. 2, pp. 907–19, 2014. doi:10.1109/TVT.2013.2294032

4. X. Li, J. Tan, A. Liu, P. Vijayakumar, N. Kumar, and M. Alazab, "A novel UAV-enabled data collection scheme for intelligent transportation system through UAV speed control," *IEEE Trans. Intell. Transp. Syst.*, Vol. 22, no. 4, pp. 2100–10, 2021. doi:10.1109/TITS.2020.3040557

5. Dedicated Short Range Communications (DSRC), [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html.

6. M. Raya, and J. P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, Vol. 15, no. 1, pp. 39–68, 2007. doi:10.3233/JCS-2007-15103

7. M. S. Bouassida, "Authentication vs. privacy within vehicular ad hoc networks," *Int. J. Netwo Secur.*, Vol. 13, no. 3, pp. 121–34, 2011.

8. R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen. "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. 27th Conf. Comput. Commun. (INFOCOM)*, Phoenix, USA, pp. 1229–37, 2008.

9. M. Azees, P. Vijayakumar, and L. J. Deborah, "Eaap: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, Vol. 18, no. 9, pp. 2467–76, 2017. doi:10.1109/TITS.2016.2634623

10. X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "Tsvc: timed efficient and secure vehicular communications with privacy preserving," *IEEE Trans. Wireless Commun.*, Vol. 7, no. 12, pp. 4987–98, 2008. doi:10.1109/T-WC.2008.070773

11. C.-C. Chang, J.-H. Yang, and Y.-C. Wu, "An efficient and practical authenticated communication scheme for vehicular ad hoc networks," *Int. J. Netwo Secur.*, Vol. 17, no. 6, pp. 702–7, 2015.

12. C.-C. Lee, Y.-M. Lai, and P.-J. Cheng. An efficient multiple session key establishment scheme for VANET group integration," in 2015 *IEEE Intelligent Vehicles Symposium (IV)*, Seoul, Korea, pp. 1316–21, 2015.

13. S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, and M. K. Khan, "Enhancing security and privacy for identity-based batch verification scheme in VANETs," *IEEE Trans. Veh. Technol*, Vol. 66, no. 4, pp. 3235–48, 2017. doi:10.1109/TVT.2015.2406877

14. Z. Jianhong, X. Min, and L. Liying, "On the security of a secure batch verification with group testing for VANET," *Int. J. Netwo Secur.*, Vol. 16, no. 4, pp. 313–20, 2014.

15. L. Wang, D. Zheng, R. Guo, C.-C. Hu, and C.-M. Jing, "A blockchain-based privacy-preserving authentication scheme with anonymous identity in vehicular networks," *Int. J. Netwo Secur.*, Vol. 22, no. 6, pp. 981–90, 2020.

16. A. K. Malhi, and S. Batra, "An efficient certificateless aggregate signature scheme for vehicular ad hoc networks," *Discrete Math. Theor. Comput. Sci., DMTCS*, Vol. 17, no. 1, pp. 317–38, 2015.

17. S.-J. Horng, S.-F. Tzeng, P.-H. Huang, X. Wang, T. Li, and M. K. Khan, "An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," *Inf. Sci. (Ny)*, Vol. 317, pp. 48–66, 2015. doi:10.1016/j.ins.2015.04.033

18. J. Li, H. Yuan, and Y. Zhang. Cryptanalysis and improvement of certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," *eprint, IACR, Tech. Rep.,* 2016., 2016.

19. J. Cui, J. Zhang, H. Zhong, R. Shi, and Y. Xu, "An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks," *Inf. Sci. (Ny)*, Vol. 451–452, pp. 1–15, 2018.

20. P. Kumar, and V. Sharma, "On the security of certificateless aggregate signature scheme in vehicular ad hoc networks," *Adv. Intell. Syst. and Comput., AICS*, Vol. 583, pp. 715–22, 2018.

21. X. Yang, C. Chen, T. Ma, Y. Li, and C. Wang. "An improved certificateless aggregate signature scheme for vehicular ad-hoc networks," in *Proc. IEEE 3rd Adv. Inf. Technol., Electron. Autom. Control Conf.*, 2018, pp. 2334–8.

22. P. Kumar, S. Kumari, V. Sharma, X. Li, A. K. Sungaiah, and S. K. H. Islam, "Secure CLS and CL-AS schemes designed for VANETs," *J. Supercomput*, Vol. 75, pp. 3076–98, 2019. doi:10.1007/s11227-018-2312-y

23. H. Zhong, S. Han, J. Cui, J. Zhang, and Y. Xu, "Privacy-preserving authentication scheme with full aggregation

in VANET," *Inf. Sci. (Ny)*, Vol. 476, pp. 211–21, 2019. doi:10.1016/j.ins.2018.10.021

24. I. A. Kamil, and S. O. Ogundoyin, "An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks," *J. Inform. Secur. Appl.*, Vol. 44, pp. 184–200, 2019.

25. Y. Zhao, Y. Hou, L. Wang, S. Kumari, M. K. Khan, and H. Xiong, "An efficient certificateless aggregate signature scheme for the internet of vehicles," *Trans. Emerging. Tel. Tech.*, Vol. 31, no. 5, pp. 1–20, 2019.

26. X. Hu, W. Tan, C. Yu, C. Ma, and H. Xu. Security analysis of certificateless aggregate signature scheme in VANETs," in 2019 *12th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*, Suzhou, China, 2019.

27. N. Zhao, and G. Zhang. Privacy-protected certificateless aggregate signature scheme in VANET," in 2019 *11th International Conference on Wireless Communications and Signal Processing (WCSP)*, Xi'an, China, 2019.

28. I. Ali, M. Gervais, E. Ahene, and F. Li, "A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs," *J. Syst. Archit.*, Vol. 99, 101636, 2019. doi:10.1016/j.sysarc.2019.101636

29. K. Li, M. H. Au, W. H. Ho, and Y. L. Wang, "An efficient conditional privacy-preserving authentication scheme for vehicular ad hoc networks using online/offline certificateless aggregate signature," in *Provsec 2019*, R. Steinfeld, and T. H. Yuen Eds. Springer, Cham: LNCS 11821, 2019, pp. 59–76.

30. C. Li, G. Wu, L. Xing, F. Zhu, and L. Zhao, "An efficient certificateless aggregate signature scheme designed for VANET," *Comput. Mater Continua*, Vol. 63, no. 2, pp. 725–42, 2020.

31. Z. Xu, D. He, N. Kumar, and K.-K. R. Choo, "Efficient certificateless aggregate signature scheme for performing secure routing in VANETs," *Secur. Commun. Netw.*, Vol. 2020, no. Art. no. 5276813, pp. 1–12, 2020.

32. I. A. Kamil, and S. O. Ogundoyin, "On the security of privacy-preserving authentication scheme with full aggregation in vehicular ad hoc network," *Secur. Priv.*, Vol. 3, no. 3, pp. 1–20, 2020.

33. X. Hu, W. Tan, C. Ma, and H. Xu. "Certificateless aggregate signature scheme with high efficiency in vehicular ad-hoc network," in *EITCE 2020: Proceedings of the 2020 4th International Conference on Electronic Information Technology and Computer Engineering*, Xiamen, China, 2020, pp. 1008–12.

34. Q. Mei, H. Xiong, J. Chen, M. Yang, S. Kumari, and M. K. Khan, "Efficient certificateless aggregate signature with conditional privacy preservation in IoV," *IEEE Syst. J.*, Vol. 15, no. 1, pp. 245–256, 2021.

35. B. Thumbur, G. S. Rao, P. V. Reddy, N. B. Gayathri, D. V. R. K. Reddy, and M. Padmavathamma, "Efficient and secure certificateless aggregate signature-based authentication scheme for vehicular ad hoc networks," *IEEE Internet Things J.*, Vol. 8, no. 3, pp. 1908–20, 2021. doi:10.1109/JIOT.2020.3019304

36. T. F. Vallent, D. Hanyurwimfura, and C. Mikeka, "Efficient certificate-less aggregate signature scheme with conditional privacy-preservation for vehicular ad hoc networks enhanced smart grid system," *Sensors*, Vol. 21, pp. 2900, 2021. doi:10.3390/s21092900

37. X. Ye, G. Xu, X. Cheng, Y. Li, and Z. Qin, "Certificateless-based anonymous authentication and aggregate signature scheme for vehicular ad hoc networks," *Wirel. Commun. Mob. Comput.*, Vol. 2021, pp. Article ID 6677137, 2021.

38. Y. Ren, X. Li, S.-F. Sun, X. Yuan, and X. Zhang, "Privacy-preserving batch verification signature scheme based on blockchain for vehicular ad-hoc networks," *J. Inform. Secur. Appl.*, Vol. 58, pp. 102698, 2021.

39. Y. Wang, H. Zhong, Y. Xu, and J. Cui, "Ecpb: efficient conditional privacy preserving authentication scheme supporting batch verification for VANETs," *Int. J. Netwo Secur.*, Vol. 18, no. 2, pp. 374–82, 2016.

40. S. Ibrahim, M. Hamdy, and E. Shaaban, "Towards an optimum authentication service allocation and availability in VANETs," *Int. J. Netwo Secur.*, Vol. 19, no. 6, pp. 955–65, 2017.

41. R. Castro, and R. Dahab. Efficient certificateless signatures suitable for aggregation," in *IACR Cryptology*, 2007.

42. A. Shamir, "Identity-based cryptosystem and signatures schemes," in *Advances in Cryptology – Crypto '84*, Blakley G.R., Chaum D. Eds. Springer, Berlin, Heidelberg: LNCS 196, 1984, pp. 47–53.

43. W. Yang, M.-R. Chen, and G.-Q. Zeng, "Cryptanalysis of two strongly unforgeable identity-based signatures in the standard model,"," *Int. J. Netw. Secur.*, Vol. 20, no. 6, pp. 1194–9, 2018.

44. S. S. Al-Riyami, and K. G. Paterson. Certificateless public key cryptography," in *Advances in Cryptology – ASIACRYPT* 2003, LNCS 2894, pp. 452–73, 2003.

45. G. Sharma, S. Bala, and A. K. Verma, "An improved RSA-based certificateless signature scheme for wireless sensor networks," *Int. J. Netw. Secur.*, Vol. 18, no. 1, pp. 82–9, 2016.

46. Z. Xu, D. He, P. Vijayakumar, K.-K. R. Choo, and L. Li, "Efficient NTRU lattice-based certificateless signature scheme for medical cyber-physical systems," *J. Med. Syst.*, Vol. 44, no. 92, 2020.

47. J. Xie, Y. Hu, J. Gao, W. Gao, and M. Jiang, "Efficient certificateless signature scheme on ntru lattice," *KSII Trans.*

Internet Inform. Syst., Vol. 10, no. 10, pp. 5190–208, 2016.

48. F. Qu, F.-Y. Wang, and L. Yang, "Intelligent transportation spaces: vehicles, traffic, communications, and beyond," *IEEE Commun. Mag.*, Vol. 48, no. 11, pp. 136–42, 2010. doi:10.1109/MCOM.2010.5621980

49. Y. Ming, and H. Cheng, "Efficient certificateless conditional privacy-preserving authentication scheme in VANETs," *Mob. Inf. Syst.*, Vol. 2019, pp. 1–19, 2019.

50. K.-A. Shim, "Cpas: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Trans. Veh. Technol.*, Vol. 61, no. 4, pp. 1874–83, 2013. doi:10.1109/TVT.2012.2186992

51. D. Boneh, and M. Franklin. "Identity-based encryption from the weil pairing," in *Proceedings of Crypto*, 2001, LNCS 2139, pp. 213–29.

52. A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR- reduction," *IEICE Trans. Fund*, Vol. E84, no. A, pp. 1234–43, 2001.

53. D. Boneh, B. Lynn, and H. Shacham. "Short signatures from the weil pairing," in *Proc. Asiacrypt*, 2001, LNCS 2248, pp. 514–32.

54. V. Miller. "Use of elliptic curves in cryptography," in *Proc. Adv. Cryptol. (Crypto)*, 1985, pp. 417–26.

55. N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput*, Vol. 48, no. 177, pp. 203–9, 1987. doi:10.1090/S0025-5718-1987-0866109-5

56. M. M. Rasslan, "A stamped hidden-signature scheme utilizing the elliptic curve discrete logarithm problem," *Int. J. Netw Secur.*, Vol. 13, no. 1, pp. 49–57, 2011.

57. S.-G. Liu, X. Heng, and Y.-M. Li, "Anti-SPA scalar multiplication algorithm on twisted edwards elliptic curve," *Int. J. Netw. Secur.*, Vol. 22, no. 6, pp. 1015–1021, 2020.

58. P. Vijayakumar, M. Azees, A. Kannan, and L. J. Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, Vol. 17, no. 4, pp. 1015–28, 2016. doi:10.1109/TITS.2015.2492981

59. E. F. Cahyadi, and M.-S. Hwang, "An improved efficient anonymous authentication with conditional privacy-preserving scheme for VANETs," *PLoS ONE*, Vol. 16, no. 9, pp. e0257044, 2021.

60. J. Shen, D. Liu, X. Chen, J. Li, N. Kumar, and P. Vijayakumar, "Secure real-time traffic data aggregation with batch verification for vehicular cloud in VANETs," *IEEE Trans. Veh. Technol.*, Vol. 69, no. 1, pp. 807–17, 2020. doi:10.1109/TVT.2019.2946935

61. Y.-C. Chen, and R. Tso, "A survey on security of certificateless signature schemes," *IETE Tech. Rev.*, Vol. 33, no. 2, pp. 115–21, 2015. doi:10.1080/02564602.2015.1049223

62. Y. Zhang, R. H. Deng, G. Han, and D. Zheng, "Secure smart health with privacy-aware aggregate authentication and access control in internet of things," *J. Netw. Comput. Appl.*, Vol. 123, pp. 89–100, 2018. doi:10.1016/j.jnca.2018.09.005

63. Y. Ming, and X. Shen, "Pcpa: a practical certificateless conditional privacy preserving authentication scheme for vehicular ad hoc networks," *Sensors*, Vol. 8, no. 5, pp. 1573, 2018. doi:10.3390/s18051573

64. D. Wang, and J. Teng, "Probably secure certificateless aggregate signature algorithm for vehicular ad hoc network," *J. Electronica Inf. Technol*, Vol. 40, no. 1, pp. 11–7, 2018.

65. S. O. Ogundoyin, "An autonomous lightweight conditional privacy-preserving authentication scheme with provable security for vehicular ad-hoc networks," *Int. J. Comput. Appl*, Vol. 42, pp. 1–16, 2018.

AUTHORS

Eko Fajar Cahyadi is a lecturer in the Faculty of Telecommunication and Electrical Engineering, Institut Teknologi Telkom Purwokerto, Indonesia, and currently pursuing a PhD degree in the Department of Computer Science and Information Engineering, Asia University, Taiwan. He received a BEng in electrical engineering from Institut Sains dan Teknologi Akprind Yogyakarta, Indonesia, in 2009, and subsequently an MSc degree from Institut Teknologi Bandung, Indonesia, in 2013. His research interest includes information security, mobile communications, and VANETs.

Email: ekofajarcahyadi@ittelkom-pwt.ac.id

Min-Shiang Hwang received PhD in computer and information science from National Chiao Tung University, Taiwan, in 1995. He was the chairman of the Department of Information Management, Chaoyang University of Technology and National Chung Hsing University during 1999–2009. He was also a visiting professor with the University of California, Riverside and Davis (USA) during 2009–2010. He obtained the 1997–2001 Excellent Research Award of National Science Council. Dr Hwang was the dean of College of Computer Science, Asia University (AU) during 2011–1015. He is currently a chair professor of AU. He has published over 200 articles in international journals.

Corresponding author. Email: mshwang@asia.edu.tw