Aggregatable Certificateless Designated Verifier Signature

Pairat Thorncharoensri
*University of Wollongong, pairat@uow.edu.au*

Willy Susilo
*University of Wollongong, wsusilo@uow.edu.au*

Follow this and additional works at: https://ro.uow.edu.au/eispapers1

Part of the Engineering Commons, and the Science and Technology Studies Commons

**Recommended Citation**

Thorncharoensri, Pairat and Susilo, Willy, "Aggregatable Certificateless Designated Verifier Signature" *(2020).* *Faculty of Engineering and Information Sciences - Papers: Part B.* 4069.
https://ro.uow.edu.au/eispapers1/4069

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au
Aggregatable Certificateless Designated Verifier Signature

Abstract
In recent years, the Internet of Things (IoT) devices have become increasingly deployed in many industries and generated a large amount of data that needs to be processed in a timely and efficient manner. Using aggregate signatures, it provides a secure and efficient way to handle large numbers of digital signatures with the same message. Recently, the privacy issue has been concerned about the topic of data sharing on the cloud. To provide the integrity, authenticity, authority, and privacy on the data sharing in the cloud storage, the notion of an aggregatable certificateless designated verifier signature scheme (ACLDVS) was proposed. ACLDVS also is a perfect tool to enable efficient privacy-preserving authentication systems for IoT and or the vehicular ad hoc networks (VANET). Our concrete scheme was proved to be secured underling of the Computational Diffie-Hellman assumption. Compared to other related schemes, our scheme is efficient, and the signature size is considerably short.

Keywords
verifier, designated, certificateless, signature, aggregatable

Disciplines
Engineering | Science and Technology Studies

Publication Details
Thorncharoensri, P. & Susilo, W. (2020). Aggregatable Certificateless Designated Verifier Signature. IEEE Access, 8 95019-95031.

This journal article is available at Research Online: https://ro.uow.edu.au/eispapers1/4069
**ABSTRACT** In recent years, the Internet of Things (IoT) devices have become increasingly deployed in many industries and generated a large amount of data that needs to be processed in a timely and efficient manner. Using aggregate signatures, it provides a secure and efficient way to handle large numbers of digital signatures with the same message. Recently, the privacy issue has been concerned about the topic of data sharing on the cloud. To provide the integrity, authenticity, authority, and privacy on the data sharing in the cloud storage, the notion of an aggregatable certificateless designated verifier signature scheme (ACLDVS) was proposed. ACLDVS also is a perfect tool to enable efficient privacy-preserving authentication systems for IoT and or the vehicular ad hoc networks (VANET). Our concrete scheme was proved to be underling of the Computational Diffie-Hellman assumption. Compared to other related schemes, our scheme is efficient, and the signature size is considerably short.

**INDEX TERMS** Certificateless signature, aggregate signature, designated verifier, privacy, authentication, vehicular ad hoc network (VANET), wireless sensor network (WSN).

**I. INTRODUCTION**

A wireless sensor network (WSN) is made up of a large number of sensor nodes, which are densely deployed very close to each other. It has the advantages of low cost, high efficiency and low latency. The protocols and algorithms used in the wireless sensor network must possess self-organizing capabilities. A sensor node has an onboard processor, and it can be used to process simple computations locally and transmits only the necessary and partially processed data back to the requested node. This cooperative effort of sensor nodes is one of the unique and attractive features of wireless sensor networks.

The above-described feature ensures a wide range of applications for wireless sensor networks, for example, healthcare, military, and security. For healthcare application, a doctor can securely monitor the wearable health devices. With consent from the patient, the wearable health devices allow the doctor to have a better understanding of the patient’s current condition. However, the generated patient’s medical reports from these devices could leak the privacy of the patient, and, hence, there should be appropriately handled and be protected. The data and its signature transmitting between the sensor devices and the monitor have to be encrypted to provide confidentiality and authenticity. It can be done merely implementing the SSL/TLS protocol. Nevertheless, it ensures only confidentiality and authenticity, but it does not preserve the privacy of the patient. For the privacy of a patient, it can be achieved by implement the designated verifier signature instead of the general signature. Moreover, to save the cost of the communication and computation, the aggregate signature scheme can be applied to limit the amount of the data needed to transmit through the network. The data and its signature can be gathering at the sensor gateway, then the sensor gateway aggregates them into a single signature and passes it to the monitor server. The detail of this implementation is described in [10].

With the rapid growth of the application of various Internet of Things (IoT) devices and the development of wireless communication technology especially for WSN, the topic of vehicular ad hoc networks (VANET) has attracted significant interest and attention. In VANET, Vehicles equipped wireless devices can communicate with each other. The main objective of VANET is to set up and maintain a communication network among vehicles without using any centralized network architecture based base station [26]. One of the
examples of the VANET applications, the critical medical emergencies in a place with no access to any communication infrastructure, it is vital to pass on the information that could save human lives. Lack of support in VANET, it has put additional responsibility on each vehicle that is part of the network. Every node must maintain and forward the communication on this network to other nodes. In the United State, the intelligent transportation systems (ITS) implement the Dedicated Short Range Communications (DSRC) that operates around the 5.9 GHz frequency band. The DSRC consists of RoadSide units (RSUs) and On-Board Units (OBUs) that have transceivers and transponders. A vehicle with OBUs can communicate with another vehicle with OBUs directly, which is called Vehicle to Vehicle (V2V) communication. Meanwhile, a vehicle with OBUs that communicates with a Road Side Unit (RSU) is known as Vehicle-to-Infrastructure (V2I). Each vehicle in VANET can operate in both modes of communication simultaneously. More details of VANET can be found in [25].

However, the rapid movement of the nodes affect the stability of the network route and the large scale of nodes in the network caused communication delays, is a significant problem on VANET that could not be ignored [9]. The concept of certificateless public key cryptography has been recommended to secure the communication in the VANET, and avoid the complexity associated with managing public key certificates and the drawbacks of the key escrows in identity-based cryptography [25], [26], [29], [30]. For the public key management in cryptography, Certificate Authority(CA) is commonly utilized to certify the public key. However, it is a security weak point in the VANET, which creates a single point of failure. In the VANET environments, where the perspective of limited bandwidth and the dynamic nature of the networks are crucial. A compromised AC will put the security of the whole VANET in risk, and the collapsing of the communication in the network is unavoidable. Hence, the efficient key agreement and distribution in VANET is strategically assigned to certificateless cryptography. In some specific applications, the signatures on the same message generated by different nodes need to be compressed to reduce the cost of transmission and verification computation due to the bandwidth and storage constrained environments. The above issue can be solved with an aggregate signature which can reduce the cost of verification, and the length of the signature. It was designed to be effective in the bandwidth and storage constrained environments.

A. RELATED WORK

Since the seminal introduction of digital signature notion [11] and its formalization [12], the notion of digital signatures has been extended to capture different scenarios and situations in real life. With a public-private keys pair, it allows a signer with a private key to produce a signature on the message and lets anyone verify this signature with a public key.

A designated verifier signature (DVS) provides both authenticity and deniability properties at the same time. It was proposed by Jakobsson, Sako and Impagliazzo in [19]. The authenticity property ensures that a signer indeed signs this digital signature. The deniability property ensures that only the designated verifier can verify the validity of this digital signature signed by the signer. Moreover, this conviction cannot be transferred to any other third party. It has been widely studied and extended to many areas [13], [16], [18], [21], [22], [24], [32]–[35], [37].

Laguillaumie and Vergnaud were first to propose a multi-designated verifiers signature scheme (MDVS) in [21]. Later, Thorncharoensri et al. [35] introduced a policy-controlled signature (PCS) which is a variant of MDVS in the attributed based topics. They also proposed the extension schemes in [37]. The signature size of MDVS schemes is linear to the number of the designated verifiers, while the signature size of PCS schemes is linear to the number of the attribute in the policy, but it does not limit the number of the designated verifiers. There are many variants of DVS, such as the universal designated verifier signature (UDVS) scheme [32], [36] where a delegator can sign on behalf of the signer, the one-time UDVS scheme where a signature can be recover if the delegator produced more than one universal designated verifier signature, ID-based DVS [33], and proxy DVS [16].

The certificateless public key cryptography was first proposed by Al-Riyami and Paterson in [2]. Unlike the traditional public key cryptography that needs a certificate to ensure the authenticity of the public keys, certificateless public key cryptography does not require the use of any certificate. The formal security definitions of certificateless signature (CLS) schemes have been intensively discussed by Au et al. in [3], Huang et al. in [15] and Huang et al. in [17]. Karati et al. [20] put forward the lightweight certificateless signature that can be run on restricted computation devices. However, it was proven to be insecure by Zhang et al. [39]. Later, Yang et al. [38] illustrates the public key replacement attack on the Zhang et al.’s improved CLS scheme [39].

The used of certificateless aggregate signature on VANETs application was demonstrated by Cui et al. [9]. They also proposed an efficient certificateless aggregate signature scheme for the VANETs which does not require bilinear pairing. The certificateless public key cryptography in the standard model was proposed by Canard and Trinh in [7].

In some applications such as Multicast applications which may allow data sending from the leaf nodes to gather at the branch node before pass to the root node. This leads to a many-to-one communication pattern. To ensure authenticity, integrity and non-repudiation, the cost of verification computation and bandwidth is linear to the size of the leaf nodes. This leads to the propose of the aggregate signature scheme in 2003 by Boneh et al. [6]. An aggregate signature refers to an aggregation of n signatures of n messages signed by n signers, by an aggregation algorithm, into a single signature. The verifier only needs to verify this aggregate signature, which confirms whether or not the signature is from the specified n users. Aggregate signatures not only
reduce the cost of verification but can also reduce the length of the signature that is transmitted and can be valuable in environments constrained for bandwidth and storage. Since the proposed of the aggregate signature scheme, it has been widely studied and expanded in many areas. Recently, due to the popularity of the IoT topics, the compact and lightweight certificateless aggregate signature schemes were proposed in [10], [14], [23]. Deng et al. proposed a certificateless short aggregate signature in [10]. It is efficient in the signing and verifying process where requires only two pairing operations in the verification, and the size of the signature is only one point on the elliptic curve and some state of information. However, the state of information must be shared among signers (devices) before each signer can sign on a message. This causes another issue in securely generated a shared state of information. Hashimoto and Ogata introduced a compact and unrestricted certificateless aggregate signature which the signature’s size is constant. Their concrete scheme shares the similarity to Deng et al.’s concrete scheme; however, the former scheme is much flexible. It does not need to share a state of information for every time the signer generates a signature. Li et al. recently proposed the most efficient certificateless aggregate signature scheme in [23]. The concrete scheme does not require the bilinear pairing, and it also allowed the scalar multiplication over $E/F_q$ to be computed offline and store them for later use. Therefore, it is suitable for limited computation power IoT devices.

Huang et al. was first introduced the notion of certificateless designated verifier signature schemes in [18]. Recently, many certificateless designated verifier signature schemes were proposed [13], [22], [28], [31]. Rastegari et al. [28] provided intensive security reviews on certificateless designated verifier signature schemes and they gave a conclusion on the suitable security model for certificateless designated verifier signature schemes. They also proposed a concrete scheme in a standard model. Shen et al. introduced the certificateless aggregate signature with the designated verifier (CLASSDV) in [31]. In this scheme, the aggregator acts as a delegator in the universal designated verifier signature scheme which, given a signature from the original signer, he/she can generate a designated verifier signature on behalf of the original signer. Unlike the aggregator in our scheme, he/she can only aggregate the signature to reduce the communication cost and cannot generate a designated verifier on behalf of the signers.

Our goal to construct the aggregatable certificateless designated verifier signature scheme (ACLUDVS) is not a simple task by combining or modifying the above-mentioned works. There is no generic DVS scheme that can convert an existing DVS scheme to ACLUDVS. Combining certificateless signature, aggregate signature and designated verifier signature together is not a trivial process. For example, in Shen et al. CLASSDV scheme [31], it can only achieve privacy through the aggregator. The privacy of the signer is not preserved since the beginning.

Since our scheme is unique and applicable for many applications, our comparison with other schemes is aims to compare in term of performance. Our scheme position in the balance of communication cost, performance and privacy-preserving. Hence, the well-known related signature schemes [9], [18], [20] were chosen for the comparison in Section V.

B. OUR CONTRIBUTIONS

In this paper, we concentrate on providing a designated verifier signature that can simultaneously aggregate by any party; however, only the designated verifier can prove the validity of this aggregate designated verifier signature.

Our reliable and efficient certificateless aggregate designated verifier scheme solves the aforementioned problems in integrity, authentication, and privacy. Compared with other certificateless aggregate signature and certificateless designated verifier schemes, our scheme has better performance as follows.

1) Our concrete scheme does not employ expensive bilinear pairings and map-to-point hash functions, hence, our scheme can easily implement on most of IoT devices. Since our scheme has a unique property that it is a combination of aggregate signature, designated verifier signature and certificate less signature schemes, we compared our scheme to well known efficient schemes in those areas. The results of the comparison are in the Table 2 and Figure 1 to 5.

2) Our concrete scheme satisfies the requirements of unforgeability in [28] as we demonstrated our security proofs in Section IV-A.

3) Our concrete scheme provides a signer privacy preservation in the aspect of deniability; hence, none other than designated verifier can verify the validity of the signature. This property is due to the transcript simulation, which it is indicated that the designated verifier can also generate the signature.

Paper Organization: The organization of the paper is organized as follows. In the next section, some notation and definitions used throughout this paper is described. The definition of an aggregatable certificateless designated verifier signature (ACLUDVS) and its security notions are described in Section III. In the following section, the construction of the efficient ACLUDVS scheme is described with its security proof. Finally, the comparison of our scheme with other schemes and the conclusion of the paper will be presented in the last two sections.

II. PRELIMINARIES

A. NOTATION

The following notations will be used in the rest of this paper. A function $f : \mathbb{N} \rightarrow \mathbb{R}$ is negligible when, for all constant $c > 0$ and for all sufficiently large $n$, $f(n) < \frac{1}{n^c}$. $\text{poly}(\cdot)$ is a deterministic polynomial function. Let $[n]$ represent a series of numbers(or indexes), e.g., if $n$ is integer then $[n] = \{0, \ldots, n\}$. Hence, for all polynomials $\text{poly}(k)$ and for all sufficiently large $k$, we say that $q$ is polynomial-time in $k$ if
q ≤ poly(1^k). Denote by $l \overset{S}{\leftarrow} L$ the operation of picking $l$ at random from a (finite) set $L$. Let $H : \{0, 1\}^* \to G_1$ be a collision-resistant hash function. Let $h : \{0, 1\}^* \to \mathbb{Z}_p^*$ be a collision-resistant hash function. Let $e$ be the base of the Natural Logarithms.

B. BILINEAR PAIRING

Let $G_1$ and $G_2$ be the cyclic multiplicative groups where their generators are $g_1$ and $g_2$ respectively. Let $p$ be a prime and the order of both generators. Let $G_T$ be another cyclic multiplicative group with the same order $p$. Let $\hat{e}$ be an efficient algorithm. We denote by $\hat{e} : G_1 \times G_2 \to G_T$ a bilinear mapping with the following properties:

1. Bilinearity: $\forall (g_1 \in G_1; g_2 \in G_2; a, b \in \mathbb{Z}_p) : \hat{e}(g_1^a, g_2^b) = \hat{e}(g_1, g_2)^{ab}$
2. Non-degeneracy: $\exists g_1 \in G_1 \exists g_2 \in G_2 : \hat{e}(g_1, g_2) \neq 1$.
3. Computability: $\exists \hat{e} : \forall g_1 \in G_1, \forall g_2 \in G_2: \hat{e}(g_1, g_2) \in G_T$

Note that there exists $\varphi(.)$ function which maps $G_1$ to $G_2$ or vice versa in one-unit time.

C. COMPLEXITY ASSUMPTIONS

Definition 1 (Computational Diffie-Hellman (CDH) Problem): Given a 3-tuple $(g, g^x, g^y) \in G_1$ as input, output $g^{xy}$. An algorithm $A$ has advantage $\epsilon'$ in solving the CDH problem if

$$\text{Pr}[A(g, g^x, g^y) = g^{xy}] \geq \epsilon'$$

where the probability is over the random choice of $x, y \in \mathbb{Z}_q$ and the random bits consumed by $A$.

Assumption 1 (Computational Diffie-Hellman Assumption [5, 111]): We say that the $(t, \epsilon')$-CDH assumption holds if no PPT algorithm with time complexity $t(.)$ has an advantage at least $\epsilon'$ in solving the CDH problem.

III. AGGREGATABLE CERTIFICATELESS DESIGNATED VERIFIER SIGNATURE SCHEMES (ACLDVS)

In this section we will propose our aggregatable certificateless designated verifier signature schemes (ACLDVS). There are three main players which are a trusted authority $KGC$ who issues keys associated with its public key to the rest, a verifier $V$ and a signer $S$ who generates a signature that can be verified only by a specified verifier $V$. Let $\mathbb{ID} = \{ID_1, \ldots, ID_n\}$ be a set of $n$ identities and $\mathbb{U} = \mathbb{ID} \cup \{pk_i : ID_i \in \mathbb{ID}\}$ be a set of identity and public key of $n$ users.

System Parameter Generation (Setup):

Given a security parameter $\ell$ as input, a probabilistic algorithm $\text{Setup}$ outputs the system parameter $\text{param}$ and the private key $(sk_K)$ of a trusted authority. That is,

$$\text{Setup}(\ell) \rightarrow \text{param}, sk_K.$$  

Extract Partial Private Key (PPK):

Given $\text{param}$, a user identity $ID_U \in \{0, 1\}^*$ and $sk_K$ as input, a probabilistic algorithm $\text{PPK}$ outputs the partial private key $(psk_U)$ and the public parameter $(ppk_U)$ of a user. That is,

$$\text{PPK}(\text{param}, ID_U, sk_K) \rightarrow (ppk_U, psk_U).$$

Noted that $U$ is represented the user who may be a signer or a verifier.

Setup User Secret Value (SetSV):

Given $\text{param}$ and a user identity $ID_U$ as input, a probabilistic algorithm $\text{SetSV}$ outputs the Secret Value $(sv_U)$ of the user. That is,

$$\text{SetSV}(\text{param}, ID_U) \rightarrow sv_U.$$  

Setup User Private Key (SetSK):

Given $\text{param}$, the user identity $ID_U$, $psk_U$ and $sv_U$ as input, a probabilistic algorithm $\text{SetSK}$ outputs the private key $(sk_U)$ of the user. That is,

$$\text{SetSK}(\text{param}, ID_U, psk_U, sv_U) \rightarrow sk_U.$$  

Setup User Public Key (SetPK):

Given $\text{param}$ and the user identity $ID_U$ as input, a probabilistic algorithm $\text{SetPK}$ outputs the public key $(pk_U)$ of a signer. That is,

$$\text{SetPK}(\text{param}, ID_U) \rightarrow (pk_U).$$

Signature Signing (Sign):

Given $\text{param}$, $sk_S$, $pk_S$, and a message $M$ as input, a probabilistic algorithm $\text{Sign}$ outputs a signer’s signature $\delta$. That is,

$$\text{Sign}(\text{param}, M, sk_S, pk_S) \rightarrow \delta.$$  

Aggregate (Aggregate):

Given $\text{param}$, $\delta_1, \ldots, \delta_n$ and $M$ as input, a probabilistic algorithm $\text{Aggregate}$ outputs a signer’s signature $\sigma$. That is,

$$\text{Aggregate}(\text{param}, M, \delta_1, \ldots, \delta_n) \rightarrow \sigma.$$  

Verification (Verify):

Given $\text{param}$, $sk_V$, $M$ and $\sigma$ as input, a deterministic algorithm $\text{Verify}$ outputs a verification decision $d \in \{\text{accept}, \text{reject}\}$. That is,

$$\text{Verify}(\text{param}, M, \sigma, sk_V) \rightarrow d.$$  

Transcript Simulation (Sim):

Given $\text{param}$, $sk_V$, $M$ as input, a probabilistic algorithm $\text{Sim}$ outputs a simulated signature $\sigma$. That is,

$$\text{Sim}(\text{param}, M, \sigma, sk_V) \rightarrow \hat{\sigma}.$$  

A. SECURITY MODEL OF AGGREGATABLE CERTIFICATELESS DESIGNATED VERIFIER SIGNATURE SCHEMES

In ACLDVS, there are two models of the attack which describe with different capabilities:

Type I: In this type of the attack, an adversary $A_I$ does not have access to the master key. However, it has an
ability to replace any public key and/or obtain the most of signers’ secret keys (but at least one signer’s secret key and one verifier’s secret key must remain secret to \(A_i\)). Given the above ability with the public parameter and queries in Table 1, \(A_i\) can choose messages with adaptive strategies and submit them to the signing oracle. Finally, if \(A_i\) can output a valid message-signature pair that have never been queried before, then \(A_i\) is successful in the attack.

Type II: In this type of the attack, an adversary \(A_{II}\) has access to the master key. However, it doesn’t have an ability to replace any public key of its own choice. Given the above ability with the public parameter and queries in Table 1, \(A_i\) can choose messages with adaptive strategies and submit them to the signing oracle. Finally, if \(A_i\) can output a valid message-signature pair that have never been queried before, then \(A_i\) is successful in the attack.

### IV. OUR SCHEME

The ACLDVS scheme is described as follows.

**Setup:** On input a security parameter \(\ell\), \(KGC\) randomly chooses a prime \(p \approx poly(\ell)\). Let \(G_1, G_2\) and \(G_T\) denote three groups of prime order \(p\). Let \(\hat{\ell}\) be the bilinear mapping function, which maps \(G_1\) and \(G_2\) to \(G_T\). The above mapping function is defined as \(\hat{\ell} : G_1 \times G_2 \rightarrow G_T\). To generate a public parameter, first, select a random integer \(a \in \mathbb{Z}_p^*\). Choose a random generator \(g \in G_1\) and a bilinear mapping function \(\hat{\ell}\). Construct a function \(\varphi : G_1 \rightarrow G_2\) and compute \(o = \varphi(g) \in G_2\). Select hash functions \(H : \{0,1\}^* \rightarrow G_1\) and \(h : \{0,1\}^* \rightarrow \mathbb{Z}_p^*\). Compute \(W = g^a\). Set \(sk_K = a\) and \(\text{param} = (\hat{\ell}, \varphi, o, \hat{\ell}, W, h, h)\). Then, **Setup** returns \((\text{param}, sk_K)\).

**PPK:** With \(\text{param}, sk_K\) and \(ID_U \in \{0,1\}^*\) as input, **PPK** randomly generates \(psk_U\) as follows: select random an integer \(\mu_U \in \mathbb{Z}_p^*\). Let \(ppk_U = (T_U = g^{\mu_U})\) and compute \(l_U = h(ID_U || T_U)\). Let \(psk_U = d_U = \mu_U + l_U \cdot a\). Then, **PPK** returns \((ppk_U, psk_U)\).

**SetSV:** With \(\text{param}\) and \(ID_U \in \{0,1\}^*\) as input, **SetSV** randomly generates \(sv_U\) as follows: select random integers \(x_U, y_U, z_U \in \mathbb{Z}_p^*\) and set \(sv_U = (x_U, y_U, z_U)\).

**SetSK:** With \(\text{param}, sv_U, psk_U\) and \(ID_U \in \{0,1\}^*\) as input, **SetSK** sets \(sk_U = (x_U, y_U, z_U, d_U)\).

**SetPK:** With \(\text{param}, ppk_U, sv_U\) and \(ID_U \in \{0,1\}^*\) as input, **SetPK** randomly selects an integer \(\eta \in \mathbb{Z}_p^*\). Let \(X_U = g^{\eta_U}, Y_U = g^{\delta_U}, Z_U = g^{\gamma_U}\). Next, it computes \(B_U = g^{\delta_U}Y_U = h(ID_U || [B_U || T_U || X_U || Y_U || Z_U]), C_U = \eta_U + d_U \cdot \gamma_U\). Finally, it outputs \(pk_U = (X_U, Y_U, Z_U, T_U, B_U, C_U)\) for a user \(U\).

**Sign:** With \(\text{param}, sk_S, pk_V, ID_S \in \{0,1\}^*\) and \(M \in \{0,1\}^*\) as input, **Sign** randomly generates a signature \(\sigma\) on message \(M\) as follows:

1. Select random integers \(r_S \in \mathbb{Z}_p^*\).
2. Verify \(pk_V\) by computing \(\gamma_V = h(ID_V || B_V || T_V || X_V || Y_V, Z_V)\) and checking whether \(g^{\gamma_V} = Y_VB_V^{-1} \cdot (T_V \cdot W_V)^{\gamma_V}\).
3. Compute \(l_V = h(ID_V || T_V)\).
4. Compute \(R_S = g^{\delta_S}; \hat{R}_S = h(m || R_S || X_V, Y_V, Z_V)\).
5. \(\hat{R}_S = (T_V \cdot W_V)^{\gamma_S} \cdot Z_V^{\delta_S}d_S\).
6. Compute \(\alpha_S = h(m || R_S || X_V, Y_V, Z_V)pk_S\).
7. \(\hat{\sigma} = Y_V^{-\delta_S} \cdot \hat{R}_S \cdot X_V^{\alpha_S}d_S\).
8. \(\sigma = \hat{\sigma} \bmod p\).

**Aggregate:** Let \(R = \{R_1, \ldots, R_n\}\). With \(\text{param}, \sigma, \delta_1, \ldots, \delta_n\) and \(M \in \{0,1\}^*\) as input, **Aggregate** generates a signature \(\sigma\) on message \(M\) as follows:

\[
\sigma = \left(\prod_{i=1}^{n} \tilde{\delta}_i \right) \mod p.
\]

**Verify:** With \(\text{param}, \sigma, \delta_1, \ldots, \delta_n, sk_V\) and \(ID_V \in \{0,1\}^*\) as input, **Verify** checks whether the below equations hold or not.

1. Compute \(l_V = h(ID_V || T_V)\) for \(ID_V \in \{0,1\}^*\).
2. Verify \(pk_V\) by computing \(\gamma_V = h(ID_V || B_V || T_V || X_V || Y_V, Z_V)\) and checking whether \(g^{\gamma_V} = Y_VB_V^{-1} \cdot (T_V \cdot W_V)^{\gamma_V}\).
3. \(\hat{R}_S = h(m || R_S || X_V, Y_V, Z_V)pk_S\).
4. \(R_S = \left(\prod_{i=1}^{n} R_i \cdot W_V^{\gamma_V} \right) \mod p\).
5. \(\alpha_S = h(m || R_S || X_V, Y_V, Z_V)pk_S\).
6. Compute \(\hat{\sigma} = \left(\prod_{i=1}^{n} \tilde{\delta}_i \cdot \hat{R}_S \cdot X_V^{\alpha_S} \right) \mod p\).

If it does not hold, then **Verify** outputs reject. Otherwise, it outputs accept.

**Sim:** With \(\text{param}, \sigma, sk_V\) and \(ID_V \in \{0,1\}^*\) as input, **Sim** randomly generates a signature \(\sigma\) on message \(M\) as follows:

1. Select random integers \(r_1, \ldots, r_n \in \mathbb{Z}_p^*\).
2. Compute \(l_V = h(ID_V || T_V)\) for \(ID_V \in \{0,1\}^*\).

**Table 1. Queries.**

| Queries | meaning |
|---------|---------|
| Hash – Q | a hash query |
| PPK – Q | a partial private key query \(PPK: ID_i \rightarrow (ppk_i, psk_i)\) |
| SV – Q | a secret key query \(SV: ID_i \rightarrow s_k_i\) |
| SK – Q | a secret key query \(SK: ID_i \rightarrow sk_i\) |
| PK – Q | a public key query \(PK: ID_i \rightarrow pk_i\) |
| RPK – Q | a public key replacing (updating) query that on given input \((ID_i, pk_i)\) and it replaces \(pk_i\) with \(pk_{\hat{i}}\) |
| Sign – Q | a signature query \(Sign: (ID_S, ID_V, M) \rightarrow \sigma\) |
| Verify – Q | a signature verification query \(Verify: Q: (M, U, \sigma) \rightarrow \{0,1\}\) |
3) Verify each $p_k_i$ by computing $\gamma_i = h(ID_i||B_i||T_i||X_i||Y_i||Z_i)$ and checking whether $g^{\gamma_i} = B_i^i (T_i \cdot W_i^h)^{\gamma_i}$.
4) Compute $R_i = g^{\gamma_i} \cdot \text{VID}_i \in U$, $\text{VID}_i$ which are the secret key of the designated verifier. From the Sim algorithm, the designated verifier also can generate a valid signature by using his/her secret key ($x_U, y_U, z_U, d_U$). Hence, the signature produced by the designated verifier is indistinguishable from the signature produced by the signer. To be precise, this signature cannot confirm its validity by a third party. □

A. SECURITY ANALYSIS

Theorem 1: The ACLDVS scheme is designated verifier signature scheme.

Proof: The verification of ACLDVS requires $x_U, y_U, z_U$ and $d_U$ which are the secret key of the designated verifier. From the Sim algorithm, the designated verifier also can generate a valid signature by using his/her secret key ($x_U, y_U, z_U, d_U$). Hence, the signature produced by the designated verifier is indistinguishable from the signature produced by the signer. To be precise, this signature cannot confirm its validity by a third party.

Theorem 2: The ACLDVS scheme is existentially unforgeable under Type-I adversary $A_I$ attack model, if the CDH assumption holds in the random oracle model.

Proof: Assume that there exists a forger algorithm $A_I$ running the existential unforgeability game defined in Section III-A. Then we will show that, by using $A_I$, an adversary $F$ solves the CDH problem.

Initialization: on input $g, g^x$ and $g^y$ as an instance of the CDH problem, $F$ runs Setup and sets $g = g, W = g^x$ and obtains $(\text{param} = (p, e, g, \alpha, W, h), \text{sk}_K = \chi)$.

Queries: The following queries are constructed by $A_I$ before running the simulation.

Hash – Q : On a request for a hash value of a string $\Gamma$ ($h(\Gamma)$), $\text{Hash – Q}$ check whether $\Gamma$ in the queried list or not. If it exists in the list then return the corresponding value, otherwise, $\text{Hash – Q}$ randomly chooses $t \leftarrow Z_\mu$, then returns $h(\Gamma) = t$. $\text{Hash – Q}$ keeps $(\Gamma, t)$ in its list and the list can be accessed only by $F$. Let $q_H$ be a number of the hash queries.

PPK – Q : With $ID_i \in \{0, 1\}^*$ as input, $\text{PPK – Q}$ randomly generates $p_{sk} = \text{sk}$ as follows: select random integers $\mu_i, l_i \in Z_\mu$. Let $p_{sk} = (T_i = g^{l_i-\text{sk}(X_i)})$ and set $h(ID_i||T_i) = l_i$. $\text{PPK – Q}$ outputs $p_{sk} = d_i = \mu_i$.

SV – Q : With $ID_i \in \{0, 1\}^*$ as input, $\text{SV – Q}$ selects random integers $x_i, y_i, z_i \in Z_\mu$, sets $\text{sv}_i = (x_i, y_i, z_i)$. Then, $\text{SK – Q}$ returns $\text{sv}_i$ for $ID_i$. However, if the input identity is $ID'_V$, it will abort the simulation. $\text{SK – Q}$ is the list of queried $ID_i$ in the $\text{PPK – Q}$ queries. $\text{PPK – Q}$ returns $(\text{ppk}_U, \text{ppsk}_U)$.

SV – Q : With $ID_i \in \{0, 1\}^*$ as input, $\text{SV – Q}$ selects random integers $x_i, y_i, z_i \in Z_\mu$, sets $\text{sv}_i = (x_i, y_i, z_i)$. Then, $\text{SK – Q}$ returns $\text{sv}_i$ for $ID_i$. However, if the input identity is $ID'_V$, it will abort the simulation. Let $q_S$ be a number of the queries with the $ID_i$ in the list $L_{sk}$.

$\text{SK – Q}$: Since $\text{PPK – Q}$ and $\text{SV – Q}$ queries can be used to obtain the same result with this type of query, hence, for this attack model, we simply ignore its construction.

PK – Q : With $ID_i \in \{0, 1\}^*$ as input, $\text{PK – Q}$ runs SetPK to output $p_{sk} = (X_i = g^{x_i}, Y_i = o^{y_i}, Z_i = o^{z_i}, T_i)$ for a user $U$. However, if the input identity is $ID'_V$, it randomly picks $x_{SV}, y_{SV}, x_{SV}, y_{SV}, z_{SV} \in Z_\mu$, sets $\text{sv}_i = (x_{SV}, y_{SV}, z_{SV})$ in $\text{Hash – Q}$ and calculates $B_{SV} = g^{x_{SV}} (T_{SV} \cdot W_{SV})^{\gamma_{SV}}$, $\text{sv}_i = (x_{SV}, y_{SV}, z_{SV})$ for $ID'_V$. Let $q_{pk}$ be a number of the queries with the $ID_i$ in the list $L_{pk}$.

RPPK – Q : With $ID_i \in \{0, 1\}^*$ and $p_{sk}$ as input, $\text{RPPK – Q}$ uses $ID_i$ to get the corresponding $p_{sk}$ from $\text{SetPK}$ and replaces it with $p_{sk}$. In order for $p_{sk}$ to pass the public key verification, $\text{RPPK – Q}$ recomputes $T_i, B_i, c_i$ for $p_{sk}$. However, for $ID'_V$, $\text{RPPK – Q}$ randomly chooses $k_i, j_i \in Z_\mu$, sets $\gamma_i = k_i + \text{hash}(ID_i||B_i||T_i||X_i||Y_i||Z_i)$ and calculates $B_i = g^{(T_{SV} \cdot W_{SV})^{k_i}}$, $c_i = j_i$. The list $L_{rk}$ keeps $(ID_i, p_{sk}, p_{sk})$.

Sign – Q : With $M \in \{0, 1\}^*$, $ID_V$ and $U$ as input, $\text{Sign – Q}$ runs $\text{Sig}$ or $\text{Sim}$ for all signature queries except a signature query for $ID'_V$ as a signer and $ID'_V$ as a verifier. $\text{Sign – Q}$ outputs the signature for $ID'_V$ as a signer and $ID'_V$ as follows:

1) Select random integers $i_{S_{SV}} \in Z_\mu$.
2) Verify $p_{sk}$ by computing $\gamma_i = h(ID_i||B_i||T_i||X_i||Y_i||Z_i)$ and checking whether $g^{\gamma_i} = B_i^i (T_i \cdot W_i^h)^{\gamma_i}$.
3) Run $\text{Hash – Q}$ to obtain $l_{SV} = h(ID_{SV}||T_{SV}||X_{SV}||Y_{SV}||Z_{SV})$ and checking whether $g^{l_{SV}} = B_{SV} (T_{SV} \cdot W_{SV})^{l_{SV}}$.
4) Let $\tilde{r}_{SV} = \text{hash}(ID_{SV}||T_{SV}||X_{SV}||Y_{SV}||Z_{SV})$.
5) $R_{SV} = g^{r_{SV}}$.
6) $\tilde{r}_{SV} = h(ID_{SV}||T_{SV}||X_{SV}||Y_{SV}||Z_{SV})(\text{ppk}_{SV})(\text{ppsk}_{SV})$.
7) $\tilde{r}_{SV} = (T_{SV} \cdot W_{SV})^{l_{SV}}$, $Z_{SV}^{r_{SV}}$, $y_{SV}^{r_{SV}}$, $x_{SV}^{r_{SV}}$.
8) $\tilde{r}_{SV} = (T_{SV} \cdot W_{SV})^{l_{SV}}$, $Z_{SV}^{r_{SV}}$, $y_{SV}^{r_{SV}}$, $x_{SV}^{r_{SV}}$.
9) Output a signature $\sigma = (\tilde{r}_{SV}, R_i)$.
A technique in [4], [27] is applied. The success probability ADV_EUF–CMA(*) that \( \mathcal{A}_T \) wins the above simulation and \( \epsilon_C \) the success probability ADV_{CDH}(U) that \( \mathcal{F} \) solves the CDH problem. The success probability in solving CDH problem by using \( \mathcal{A}_I \) is based on the Forking Lemma in [4], [27]. Some notation will be defined first.

\( \epsilon_A : \) The success probability ADV_{\mathcal{A}_I}() that \( \mathcal{A}_I \) outputs a forgery.

\( \epsilon_F : \) The success probability ADV_{EUF–CMA}() that \( \mathcal{A}_I \) wins the above simulation.

\( \epsilon_C : \) The success probability ADV_{CDH}(U) that \( \mathcal{F} \) solves the CDH problem.

\( \xi_1 : \) The simulation does not abort in PPK – Q queries

\( \xi_2 : \) The simulation does not abort in SV – Q queries

\( \xi_3 : \) The simulation does not abort in RPK – Q queries

\( \xi_4 : \) The simulation does not abort after \( \mathcal{A}_I \) outputs the forgery

Noted that it is a fact that \( q_H \gg q_t \approx q_{pp} \approx q_{sv} \approx q_{pk} \) from the nature of the aforementioned simulation. The success probability in solving CDH problem is described as follows:

\[
\epsilon_F = \epsilon_A \cdot {\Pr}[\xi_1 | [\xi_2 | [\xi_3 | [\xi_4]]]]
\]

\[
= \epsilon_A \cdot \left( 1 - \frac{1}{q_{pp} + 1} \right) q_{pp} \cdot \left( 1 - \frac{1}{q_{sv} + 1} \right) q_{sv}
\]

\[
= \epsilon_A \cdot e \cdot \left( q_{pp} + 1 \right) \cdot e \cdot \left( q_{sv} + 1 \right)
\]

\[
= \epsilon_A \cdot \frac{q_{pp}}{e \cdot (q_{pp} + 1)} \cdot \frac{q_{sv}}{e \cdot (q_{sv} + 1)}
\]

\[
\geq \epsilon_A \cdot \frac{q_{H}}{e \cdot (Q_H + 1)} \cdot \frac{q_{H}}{e \cdot (Q_H - 1)}
\]

\[
\approx \epsilon_A \cdot \frac{q_{H}^{3}}{e^{3} \cdot q_{pk}}
\]

\[
\therefore \epsilon_F \approx \frac{\epsilon_A}{e^{3} \cdot q_{pk}}
\]
\[
\epsilon_C \geq \text{frk} \geq \text{acc} \frac{\epsilon_H}{\text{frk}} - \frac{1}{2^{\ell}}
\]
\[
\text{frk} \geq \epsilon_F \left( \frac{\epsilon_H}{\text{frk}} - \frac{1}{2^{\ell}} \right)
\]
\[
\text{frk} \geq \epsilon_F^2 - \frac{\epsilon_F}{2^{\ell}}
\]
\[
\text{frk} > \frac{\epsilon_F^2}{\epsilon_H}
\]
\[
\epsilon_C > \frac{\epsilon_F^2}{\epsilon_H}
\]
\[
\therefore \epsilon_F < \sqrt{\epsilon_H \epsilon_C}
\]

From (1) and (2),
\[
\frac{\epsilon_A}{\epsilon_H} \leq \sqrt{\epsilon_H \epsilon_C}
\]
\[
\therefore \epsilon_A \approx \epsilon \cdot \epsilon_H^2 \cdot \sqrt{\epsilon_H \epsilon_C}
\]

Noted that \(\frac{\epsilon_F}{\epsilon_H}\) is negligible, hence, it is omitted. To summarize the probability, \(A_s\) wins the above game and outputs a signature \(\sigma^*\) on a message \(M^*\) with a probability of \(\epsilon_3 \cdot \epsilon_H^2 \cdot \sqrt{\epsilon_H \epsilon_C}\). The above success probability shows that our aggregatable certificateless designated verifier signature scheme secures against existentially unforgeable under an adaptive chosen message attack in the Type-I adversary model if the success probability of solving CDH problem is negligible. □

Theorem 3: The ACDLVS scheme is existentially unforgeable under Type-II adversary \(A_s\) attack model, if the CDH assumption holds in the random oracle model.

Proof: For the type-I adversary attack model, hence, the KGC secret key is compromised, hence,

Assume that there exists a forger algorithm \(A_{Hs}\) running the existential unforgeable game defined in Section III-A. Then we will show that, by using \(A_{Hs}\), an adversary \(\mathcal{F}\) solves the CDH problem.

Initialization: on input \(g, g^x\) and \(g^y\) as an instance of the CDH problem, \(\mathcal{F}\) runs Setup and sets \(g = g\) and obtains \(\text{param} = (p, \hat{e}, g, a, W, h), sk_h = a\).

Queries: The following queries are constructed by \(A_{Hs}\) before running the simulation.

**Hash – Q:** On a request for a hash value of a string \(\Gamma (h(\Gamma))\), \(\mathcal{H} – \mathcal{Q}\) check whether \(\Gamma\) in the queried list or not. If it exists in the list then return the corresponding value, otherwise, \(\mathcal{H} – \mathcal{Q}\) randomly chooses \(t \in \mathbb{Z}_p\), then returns \(h(\Gamma) = t\). \(\mathcal{H} – \mathcal{Q}\) keeps \((\Gamma, t)\) in its list and the list can be accessed only by \(\mathcal{F}\). Let \(q_{Hs}\) be a number of the hash queries.

**PPK – Q:** With \(ID_i \in \{0, 1\}\) as input, \(PPK – \mathcal{Q}\) randomly generates \(sk_i\) as follows: select random integers \(\mu_i \in \mathbb{Z}_p^\ast\) Let \(\mathcal{P PK} = (T_i = g^{\mu_i})\) and compute \(l_i = h(ID_i||T_i)\). \(PPK – \mathcal{Q}\) outputs \(sk_i = d_i = \mu_i + l_i\cdot a\). Let \(q_{pp}\) be the list of queried \(ID_i\) in the \(PPK – \mathcal{Q}\) queries. \(PPK – \mathcal{Q}\) returns \((ppk_i, sk_i)\).

**SV – Q:** With \(ID_i \in \{0, 1\}\) as input, \(SV – \mathcal{Q}\) selects random integers \(x_i, y_i, z_i \in \mathbb{Z}_p^\ast\) sets \(sv_i = (x_i, y_i, z_i)\). Then, \(SV – \mathcal{Q}\) returns \(sv_i\) for \(ID_i\). However, if the input identity is \(ID_3^x\) or \(ID_4^y\), it will abort the simulation. Let \(q_{sk}\) be a number of the queries with the \(ID_i\) in the list \(L_{sk}\).

**SK – Q:** With \(ID_i \in \{0, 1\}\) as input, \(SK – \mathcal{Q}\) selects random integers \(x_i, y_i, z_i \in \mathbb{Z}_p^\ast\), runs \(PPK – \mathcal{Q}\) to obtain \((ppk_i, sk_i)\) and \(SV – \mathcal{Q}\) to obtain \((x_i, y_i, z_i)\). Next, it sets \(sk_i = (x_i, y_i, z_i, d_i)\). Then, \(SK – \mathcal{Q}\) returns \(sk_i\) for \(ID_i\). However, if the input identity is \(ID_3^x\) or \(ID_4^y\), it aborts the simulation. Let \(q_{sk}\) be a number of the queries with the \(ID_i\) in the list \(L_{sk}\).

**PK – Q:** With \(ID_i \in \{0, 1\}\) as input, \(PK – \mathcal{Q}\) runs \(SetPK\) and outputs \(pk_i = (X_i = g^{\delta_i}, Y_i = g^{x_i}, Z_i = g^{z_i}, T_i)\) for a user \(U\). However, if the input identity is \(ID_3^x\) or \(ID_4^y\), it randomly picks \(x_i^*, y_i^*, z_i^*, r_i^*, \mu_i^*, \nu_i^*, \mu_i^*, \nu_i^*, \eta_i^* \in \mathbb{Z}_p^\ast\). Next, it computes \(B_i^* = g_0^{x_i^*} \cdot y_i^* \cdot z_i^* \cdot h(ID_3^x||T_i^*||X_i^*||Y_i^*||Z_i^*), c_{i}^* = \eta_i^* + d_i^* \cdot y_i^*\), and \(B_{i} = g_0^{x_i^*} \cdot y_i^* \cdot z_i^* \cdot h(ID_4^y||T_i^*||X_i^*||Y_i^*||Z_i^*), c_{i} = \eta_i^* + d_i^* \cdot y_i^*\). Finally, it outputs \(pk_i^* = (\sigma_{i}^*, X_{i}^*, Y_{i}^*, Z_{i}^*, T_i^*) = g_0^{x_i^*} \cdot B_{i}^*, c_{i}^*\) for a user \(s_i^*\) and \(pk_v^* = (\sigma_{i}^*, X_{i}^*, Y_{i}^*, Z_{i}^*, T_i^*) = g_0^{x_i^*} \cdot B_{i}^*, c_{i}^*, \gamma_i^*\) for a user \(V_i^*\). Let \(q_{pk}\) be a number of the queries with the \(ID_i\) in the list \(L_{pk}\).

**Sign – Q:** With \(M \in \{0, 1\}^\ast, ID_v\) and \(U\) as input, \(Sign – \mathcal{Q}\) runs \(Sign\) or \(Sim\) for all signature queries except a signature query for \(ID_3^x\) as a signer and \(ID_4^y\) as a verifier. It will compute the signature for \(ID_3^x\) as a signer and \(ID_4^y\) as follows:

1) Select random integers \(r_3^*, r_4^* \in \mathbb{Z}_p^\ast\)
2) Run \(Hash – \mathcal{Q}\) to obtain \(l_{V^*} = h(ID_{V^*}||T_{V^*})\).
3) Verify \(pk_{V}^*\) by computing \(\gamma_i = h(ID_{i}||[B_i||T_i||X_i||Y_i||Z_i])\)
   and checking whether \(g_0^{\delta_i^*} \cdot B_i \cdot (\gamma_i \cdot W_i)^{y_i} = 1\).
4) Let \(\delta_{i}^* = -(X_{i} \cdot Y_{i} \cdot Z_{i})^{y_i^{x_i^*} \cdot x_i^* \cdot z_i^*} \cdot r_i^*\).
5) \(R_{i} = g_0^{x_i^*} \cdot \gamma_i^*\).
6) \(\beta_{i}^* \cdot h(m||R_{i}||Y_{i}^*||Z_{i}^*) \) \(pk_{V}^*||pk_{i}^*\).
7) \(\tilde{R}_{i} = R_{i} \cdot Z_{i}^* \cdot \beta_{i}^* \cdot \beta_{i}^* \cdot \gamma_i^*\).
8) Set \(h(m||R_{i}||X_{i}^*||Y_{i}^*||Z_{i}^*) = \gamma_{i}^*\).
9) \(\delta_{i}^* = \gamma_{i}^* \cdot r_{i}^* \cdot R_{i} \cdot X_{i}^* \cdot r_{i}^* \cdot (x_i \cdot z_i^*)\).
   \(g = g_0^{x_i^*} \cdot (x_i \cdot z_i^*) \cdot r_i^* \cdot R_{i} \cdot X_{i}^* \cdot r_{i}^* \cdot (x_i \cdot z_i^*)\).
10) \(\delta_{i}^* = \delta_{i}^* \cdot R_{i}^*\).

**Sign – Q** outputs \(\delta_{i}^*\) for the query of a signature on \(M, ID_3^x\) and \(ID_4^y\). Let \(q_{sk}\) be a number of the queries in the list \(L_{sk}\).
$\text{Verify} - Q$ : With $M \in \{0, 1\}^*$, $\delta$, $ID_V$ and $U$ as input, $\text{Verify} - Q$ runs $\text{Verify}$ for all $ID_V$. If $ID_V$ is $ID_{V*}$ and $ID_{V*} \in U$, then check whether the below equations hold or not.

1. Run $\text{Hash} - Q$ to obtain $l_{V*} = h(ID_{V*} || T_{V*})$ and $i_l = h(ID_l || T_l) \in U$.
2. $\beta_l = h(m||R_l||Z_l||V_{\beta_l}||pk_{\beta_l}) : \forall R_l \in R$.
3. Compute $R_l = R_i \psi_i \cdot Z_l \psi_i : \forall R_l \in R$.
4. Make a query for $\alpha_l = h(m||R_l||Y_l||V_{\alpha_l}||pk_{\alpha_l}) : \forall ID_l \in U$ to $\text{Hash} - Q$.
5. Check $\hat{e}(\sigma, o) = \prod_{l=1}^{n} \hat{e}(R_l, Y_{\psi_l})$,

\[ e(\prod_{l=1}^{n} \hat{R}_l, \alpha) \cdot \prod_{l=1}^{n} \hat{e}(X_l, Z_l, X_{\psi_l})^{\alpha_l} \]

If it does not hold, then $\text{Verify}$ outputs reject. Otherwise, it outputs accept.

**Phase I:** The simulation is begun by giving $sk_k$ and an access to the above queries to $A_{II}$. Noted that $A_{II}$ always makes a query for a any string (or message) to $\text{Hash} - Q$ oracle before it outputs a potential forgery.

**Phase II:** At the end of the simulation, after executing an adaptive strategy with the above queries, $A_{II}$ outputs a forgery $\sigma^*$ on a message $M^*$ with $ID_1, \ldots, ID_n \in U^*$, $\exists ID_l \notin (L_{sk} \land L_{pp})$ and $ID_{V*} \notin (L_{sk} \land L_{pp})$. $A_{II}$ wins the game if a signature $\sigma^*$ on the message $M^*$ with $U, ID_{V*}, pk_{V*}$ is valid and it was not an output from the $\text{Sign} - Q$ queries.

**Solve CDH Problem:** To solve CHD problem, the Forking technique in [4, 27] is applied. First obtains a signature $\sigma^*$ on a message $M^*$ with $h(m||\tilde{R}_S^*||R_S^*||X_{\psi_S}^*||pk_{V*}^*||pk_{S*}^*) = \bar{r}_S$. Simultaneously $F$ resets $A_{II}$ to the initial state and repeats again the above simulation with a different hash value $h(m||\tilde{R}_S^*||R_S^*||X_{\psi_S}^*||pk_{V*}^*||pk_{S*}^*) = \bar{r}_S$. Eventually, $A_{II}$ outputs another signature $\sigma'$. Finally, $F$ compute

\[ Z = \left( \frac{\sigma^*}{\sigma} \right)^{\gamma_S} \cdot x_{V*} \cdot y_{V*} \cdot (r_S - \bar{r}_S) \]

\[ 1 = \left( \frac{x_{S*}}{\gamma_S} \right)^{\gamma_S} \cdot x_{V*} \cdot y_{V*} \cdot (r_S - \bar{r}_S) \]

\[ = \left( \frac{x_{S*}}{\gamma_S} \right)^{\gamma_S} \cdot x_{V*} \cdot y_{V*} \cdot (r_S - \bar{r}_S) \]

\[ = \left( \frac{x_{S*}}{\gamma_S} \right)^{\gamma_S} \cdot x_{V*} \cdot y_{V*} \cdot (r_S - \bar{r}_S) \]

\[ = \left( \frac{g^{x_{S*} \cdot g^{\lambda_{S*}}} \cdot g^{\psi_S^*} \cdot x_{V*} \cdot y_{V*} \cdot (r_S - \bar{r}_S)}{g^{x_{S*} \cdot g^{\lambda_{S*}}}} \right) \]

\[ = g^{x_{S*} \cdot g^{\lambda_{S*}}} \cdot g^{\psi_S^*} \]

**Probability:** Let $e_A$ be the success probability $\text{ADV}_{A_{II}}()$ that $A_{II}$ outputs a forgery. Let $e_F$ be the success probability $\text{ADV}_{EUF-CMA}()$ that $A_{II}$ wins the above simulation and $e_C$ the success probability $\text{ADV}_{CDH}()$ that $F$ solves the CDH problem. The success probability in solving CDH problem by using $A_{II}$ is based on the Forking Lemma in [4, 27]. Some notation will be defined first.

- $\epsilon_A$ : The success probability $\text{ADV}_{A_{II}}()$ that $A_{II}$ outputs a forgery.
- $\epsilon_F$ : The success probability $\text{ADV}_{EUF-CMA}()$ that $A_{II}$ wins the above simulation.
- $\epsilon_C$ : The success probability $\text{ADV}_{CDH}()$ that $F$ solves the CDH problem.

Noted that $\epsilon$ refers to the fact that $\epsilon_H \gg \epsilon_{pk} > \epsilon_{sk}$ from the nature of the aforementioned simulation. The success probability in solving CDH problem is described as follows:

\[ e_F = e_A \cdot \Pr[\epsilon_1 \mid \epsilon_2] \]

\[ = e_A \cdot (1 - \frac{1}{\epsilon_{sk} + 2})^2 \cdot \frac{1}{\epsilon_{pk} \cdot (\epsilon_{pk} - 1)} \]

\[ = \frac{e_A (\epsilon_{sk} + 1)^2}{\epsilon_{pk} \cdot (\epsilon_{pk} - 1) \cdot (\epsilon_{pk} + 2)^2} \]

\[ \approx \frac{e_A}{\epsilon_{pk}^2} \]

\[ \therefore e_F \approx \frac{e_A}{\epsilon_{pk}^2} \]

\[ e_C \geq \epsilon_{frk} \geq \Pr[\epsilon_{acc}] \cdot \frac{1}{\epsilon_H} - \frac{1}{2^l} \]

\[ \epsilon_{frk} \geq e_F \cdot \frac{\epsilon_H}{2^l} \]

\[ \epsilon_C \geq \frac{\epsilon_H^2}{2^l} \]

\[ \epsilon_C \geq \frac{\epsilon_H^2}{2^l} \]

\[ \therefore e_F < \sqrt{\frac{\epsilon_H \epsilon_C}{2^l}} \]

From (1) and (2),

\[ \frac{e_A}{\epsilon_{pk}^2} \leq \sqrt{\frac{\epsilon_H \epsilon_C}{2^l}} \]

\[ \therefore \epsilon_A \approx \epsilon_{pk}^2 \cdot \sqrt{\frac{\epsilon_H \epsilon_C}{2^l}} \]

Noted that $\frac{\epsilon_F}{2^l}$ is negligible, hence, it is omitted. To summarize the probability, $A_{II}$ wins the above game and outputs a signature $\sigma^*$ on a message $M^*$ with a probability of $e \cdot \epsilon_{pk}^2 \cdot \sqrt{\epsilon_H \epsilon_C}$. The above success probability shows that our aggregatable certificateless designated verifier signature scheme secures against existentially unforgeable under an adaptive chosen message attack in the Type-II adversary model if the success probability of solving CDH problem is negligible. \(\square\)
TABLE 2. The comparison of three certificateless signature schemes.

| Version / Size&Comp. | ACLDVS | CLAS [9] | CLDVS [18] | CLS [20] |
|----------------------|--------|----------|------------|-----------|
| $PK_K$               | $G_1$  | $2|G_1|$  | $|G_1|$     | $|G_1|+|G_1|$ |
| $SK_K$               | $|Z_p|$ | $2|Z_p|$  | $|Z_p|$     | $|Z_p|$    |
| $PK$                 | $G_1+|Z_p|$| $3|G_1|+3|Z_p|$ | $|G_1|$     | $|G_1|+|Z_p|$ |
| $SK$                 | $G_1+|Z_p|$| $2|Z_p|$  | $|G_1|$     | $2|G_1|$   |
| Signature Size       | $2|G_1|$ | $|G_1|+2|Z_p|$ | $|Z_p|$     | $2|G_1|$   |
| Sign Comp.           | $4h+11E+4M$ | $h+E$  | $h+E+M+P$ | $h+2M+2E$ |
| Verify Comp.         | $3h+12E+6M$ | $2h+3E+2M$ | $h+E+M+3P$ | $h+M+3E+P$ |

FIGURE 1. Key generation processing time.

FIGURE 2. Signature generation processing time.

V. ASYMPTOTIC ANALYSIS AND EXPERIMENTAL RESULTS

Our ACLDVS schemes captures the need of authenticity and privacy-preserving in the limited computation environment. The comparison between our scheme and other schemes in Table 2. We denoted $n$ as the number of the signers participated in the signing process for the aggregate signature scheme. Let $E$ denote a computation of exponential in $G_1$ or $G_T$. Let $M$ be a computation of scalar multiplication in $G_1$. Let $P$ be a computation of bilinear pairing function $\hat{e}$. A computation of hash functions from $\{0, 1\}^*$ to $G_1$ is denoted as $H$, and the computation of hash function from $\{0, 1\}^*$ to $\mathbb{Z}_p$ is denoted as $h$. Since the multiplication and addition computation in $\mathbb{Z}_p$ is trivial, they are omitted.

The experiments were using the Pairing-Based Cryptography Library (PBC) provided by [8]. The code was written in Python using the Charm-Crypto framework developed by Akinyele et al. [1] for the rapid cryptography.
development. The first experiment was conducted on Intel Xeon CPU model X5650 with CPU clocked at 2.67 GHz with 2 cores and 4 threads configuration with 16 Gigabytes of ECC DDR3 memory. The operating system used in this experiment is Ubuntu 18.04. The second experiment was conducted on Raspberry Pi4 Cortex-A72 (ARM v8) 64-bit
SoC with CPU clocked at 1.5 GHz with 4 cores configuration and 4 Gigabytes of DDR4 memory. Raspbian is the operation system used in the second experiment.

Both experiments were executed with 224 bit of MNT (Type D in PBC) curves. Type D curve with 224 bit size of group element is a curve that has a short size for the group elements, and it is considerably fast for the bilinear pairing computation. It achieved the security comparable to the 1344 bits (6 x 244 bits) of discrete logarithm (DLog) security.

Each experiment was conducted by first randomly selected one verifier (only for the designated verifier scheme). The number of signers participated in the simulation were start from 1 to 200 signers with a unique identity for each signer. In each round of the simulation, the number of signers participated in the signing were increased by one. In each round, the simulator ran the KGC for signers to extract the partial private-public key pair before process the key validation, signing and verification. A message used in the experiment was from 1 to 200 signers with a unique identity for each signer.

In each round of the simulation, the number of signers participated in the simulation were start from 1 to 200 signers with a unique identity for each signer. Each experiment was conducted by first randomly selected one verifier (only for the designated verifier scheme). The number of signers participated in the simulation were start from 1 to 200 signers with a unique identity for each signer. In each round of the simulation, the number of signers participated in the signing were increased by one. In each round, the simulator ran the KGC for signers to extract the partial private-public key pair before process the key validation, signing and verification. A message used in the experiment has been randomly generated in each round with a fixed size of 30 bytes. From the results in Figure 1, 2, 3, 4 and 5, our ACLDVS shows the positive result in every experiment. Even though it cannot surpass the Cui et al.’s ALCS scheme in some parts, it was significant compared to the other two schemes and benefited from the designated verifier property over the Cui et al.’s ALCS scheme.

VI. CONCLUSION

Privacy issue over the information shared in the cloud storage or in the VANET without an efficient and proper control mechanism has motivated us to provide schemes resolving it. The notion of a aggregatable certificateless designated verifier signature scheme captures the need for the integrity, authenticity, authority, and privacy, which presents as a perfect tool to enable efficient privacy-preserving authentication systems for VANET. Moreover, our ACLDVS signature is aggregatable, which it is helpful in reducing the communication cost in the ad hoc network environment.

REFERENCES

[1] J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, “Charm: A framework for rapidly prototyping cryptosystems,” J. Cryptograph. Eng., vol. 3, no. 2, pp. 111–128, Jun. 2013.

[2] S. S. Al-Riyami and K. G. Paterson, “Certificateless public key cryptography,” in Proc. 9th Int. Conf. Theory Appl. Cryptol. Inf. Secur., in Lecture Notes in Computer Science, vol. 2894. Taipei, Taiwan: Springer, Nov./Dec. 2003, pp. 452–473.

[3] M. H. Au, Y. Mu, J. Chen, D. S. Wong, J. K. Liu, and G. Yang, “Malicious KGC attacks in certificateless cryptography,” in Proc. 2nd ACM Symp. Inf., Comput. Commun. Secur. (ASIACCS), 2007, pp. 302–311.

[4] M. Bellare and G. Neven, “Multi-signatures in the plain public-key model and a general forking lemma,” in Proc. 15th ACM Conf. Comput. Commun. Secur. (CCS), Alexandria, VA, USA, 2006, pp. 390–399.

[5] D. Boneh, “The decision Diffie-Hellman problem,” in Proc. 3rd Int. Symp. Algorithmic Number Theory (ANTS), in Lecture Notes in Computer Science, vol. 1423. Portland, OR, USA: Springer-Verlag, Jun. 1998, pp. 48–63.

[6] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, “Aggregate and verifiably encrypted signatures from bilinear maps,” in Proc. Int. Conf. Theory Appl. Cryptograph. Techn., in Lecture Notes in Computer Science, vol. 2656. Warsaw, Poland: Springer, May 2003, pp. 416–432.

[7] S. Canard and V. C. Trinh, “Certificateless public key cryptography in the standard model,” Fundam. Inf., vol. 161, no. 3, pp. 219–248, Jul. 2018.

[8] A. De Caro and V. Iovino, “JPBC: Java pairing based cryptography,” in Proc. IEEE Symp. Comput. Commun. (ISCC), Corfu, Greece, Jun. 2011, pp. 850–855.

[9] 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., vols. 451–452, pp. 1–15, Jul. 2018.

[10] L. Deng, Y. Yang, and Y. Chen, “Certificateless short aggregate signature scheme for mobile devices,” IEEE Access, vol. 7, pp. 87162–87168, 2019.

[11] W. Diffie and M. Hellman, “New directions in cryptography,” IEEE Trans. Inf. Theory, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[12] S. Goldwasser, S. Micali, and R. L. Rivest, “A digital signature scheme secure against adaptive chosen-message attacks,” SIAM J. Comput., vol. 17, no. 2, pp. 281–308, Apr. 1988.

[13] S. Han, M. Xie, B. Yang, R. Lu, H. Bao, J. Lin, H.-B. Hong, M.-X. Gu, and S. Han, “A certificateless verifiable strong designated verifier signature scheme,” IEEE Access, vol. 7, pp. 126391–126408, 2019.

[14] K. Hashimoto and W. Ogata, “Unrestricted and compact certificateless aggregate signature scheme,” Inf. Sci., vol. 487, pp. 97–114, Jun. 2019.

[15] X. Huang, Y. Mu, W. Susilo, D. S. Wong, and W. Wu, “Certificateless signature revisited,” in Proc. 12th Austral. Conf. Inf. Secur. Privacy, Townsville, QLD, Australia, Jul. 2007, pp. 308–322.

[16] X. Huang, Y. Mu, W. Susilo, and F. Zhang, “Short designated verifier proxy signature from pairings,” in Proc. Workshops Embedded Ubiquitous Comput. (EUC), in Lecture Notes in Computer Science, vol. 3823. Nagasaki, Japan: Springer-Verlag, Dec. 2005, pp. 835–844.

[17] X. Huang, W. Susilo, Y. Mu, and F. Zhang, “On the security of certificateless signature schemes from Asiacrypt 2003,” in Proc. 4th Int. Conf. Cryptol. Netw. Secur., in Lecture Notes in Computer Science, vol. 3810. Xiamen, China: Springer, Dec. 2005, pp. 13–25.

[18] X. Huang, W. Susilo, Y. Mu, and F. Zhang, “Certificateless designated verifier signature schemes,” in Proc. 20th Int. Conf. Adv. Inf. Netw. Appl. (AINA), Vienna, Austria, Apr. 2006, pp. 15–19.

[19] M. Jakobsson, K. Sako, and R. Impagliazzo, “Designated verifier proofs and their applications,” in Proc. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT), in Lecture Notes in Computer Science, vol. 1070. Saragossa, Spain: Springer-Verlag, May 1996, pp. 143–154.

[20] A. Katari, S. H. Islam, and M. Karuppiiah, “Provably secure and lightweight certificateless signature scheme for IoT environments,” IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3701–3711, Aug. 2018.

[21] F. Laguillaumie and D. Vergnaud, “Multi-designated verifiers signatures: Anonymity without encryption,” Inf. Process. Lett., vol. 102, nos. 2–3, pp. 127–132, Apr. 2007.

[22] J. Li, N. Qian, Y. Zhang, and X. Huang, “An efficient certificate-based designated verifier signature scheme,” Comput. Informat., vol. 35, no. 5, pp. 1210–1230, 2016.

[23] 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 Proc. 13th Int. Conf. Prov. Secur., in Lecture Notes in Computer Science, vol. 11821. Cairns, QLD, Australia: Springer, Oct. 2019, pp. 59–76.

[24] H. Lipmaa, G. Wang, and F. Bao, “Designated verifier signature schemes: Attacks, new security notions and a new construction,” in Proc. 32nd Int. Colloq. Automat., Lang. Program. (ICALP), in Lecture Notes in Computer Science, vol. 3580. Lisbon, Portugal: Springer-Verlag, Jul. 2005, pp. 459–471.

[25] A. K. Mali, S. Batra, and H. S. Panu, “Security of vehicular ad-hoc networks: A comprehensive survey,” Comput. Secur., vol. 89, Feb. 2020, Art. no. 101664.

[26] B. Mokhtar and M. Azab, “Survey on security issues in vehicular ad hoc networks,” Alexandria Eng. J., vol. 54, no. 4, pp. 1115–1126, Dec. 2015.

[27] D. Pointcheval and J. Stern, “Security arguments for digital signatures and blind signatures,” J. Cryptol., vol. 13, no. 3, pp. 361–396, Jun. 2000.

[28] R. Rastegari, W. Susilo, and M. Dakhilalian, “Certificateless designated verifier signature revisited: Achieving a concrete scheme in the standard model,” Int. J. Inf. Secur., vol. 18, no. 5, pp. 619–635, Oct. 2019.

[29] S. Sharma and B. Kaushik, “A survey on Internet of vehicles: Applications, security issues & solutions,” Veh. Commun., vol. 20, Dec. 2019, Art. no. 100182.
[31] L. Shen, J. Ma, Y. Miao, and H. Liu, “Provably secure certificateless aggregate signature scheme with designated verifier in an improved security model,” IET Inf. Secur., vol. 13, no. 3, pp. 167–173, May 2019.

[32] R. Steinfield, L. Bull, H. Wang, and J. Pieprzyk, “Universal designated-verifier signatures,” in Proc. 9th Int. Conf. Theory Appl. Cryptol. Inf. Secur., in Lecture Notes in Computer Science, vol. 2894. Taipei, Taiwan: Springer, Nov./Dec. 2003, pp. 523–542.

[33] W. Susilo, F. Zhang, and Y. Mu, “Identity-based strong designated verifier signature schemes,” in Proc. 9th Australas. Conf. Inf. Secur. Privacy (ACISP), in Lecture Notes in Computer Science, vol. 3108. Sydney, NSW, Australia: Springer-Verlag, Jul. 2004, pp. 313–324.

[34] P. Thorncharoensri, W. Susilo, and Y. Mu, “How to balance privacy with authenticity,” in Proc. 11th Int. Conf. Inf. Secur. Cryptol., in Lecture Notes in Computer Science, vol. 5461. Seoul, South Korea: Springer, Dec. 2008, pp. 184–201.

[35] P. Thorncharoensri, W. Susilo, and Y. Mu, “Policy-controlled signatures,” in Proc. 11th Int. Conf. Inf. Commun. Secur., in Lecture Notes in Computer Science, vol. 5927. Beijing, China: Springer, Dec. 2009, pp. 91–106.

[36] P. Thorncharoensri, W. Susilo, and Y. Mu, “Universal designated verifier signatures with threshold-signers,” in Proc. 4th Int. Workshop Secur. (IWSEC), in Lecture Notes in Computer Science, vol. 5824. Toyama, Japan: Springer, Oct. 2009, pp. 89–109.

[37] P. Thorncharoensri, W. Susilo, and Y. Mu, “Policy controlled system with anonymity,” Theor. Comput. Sci., vol. 745, pp. 87–113, Oct. 2018.

[38] W. Yang, S. Wang, X. Huang, and Y. Mu, “On the security of an efficient and robust certificateless signature scheme for IoT environments,” IEEE Access, vol. 7, pp. 91074–91079, 2019.

[39] Y. Zhang, R. H. Deng, D. Zheng, J. Li, P. Wu, and J. Cao, “Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT,” IEEE Trans. Ind. Informat., vol. 15, no. 9, pp. 5099–5108, Sep. 2019.

PAIRAT THORNCHAROENSRI received the bachelor’s degree in electrical engineering from the King Mongkut’s University of Technology North Bangkok, Thailand, and the M.Sc. degree in computer science and the Ph.D. degree from the University of Wollongong (UOW), Australia. He is a Lecturer with the School of Computer Science and Information Technology and a member of the Institute of Cybersecurity and Cryptology, UOW. His main research interests are currently focused on privacy preservative techniques in the Internet of Things, blockchain, cloud computing, and big data.

WILLY SUSILO (Senior Member, IEEE) received the Ph.D. degree from the University of Wollongong (UOW), Australia, in 2001. He has been the Head of the School of Computing and Information Technology, UOW, since 2015. He was the former Head of the School of Computer Science and Software Engineering, from 2009 to 2010, and the Deputy Director of the ICT Research Institute, UOW, from 2006 to 2008. He is an innovative educator and researcher. He is a Senior Professor with the School of Computing and Information Technology, Faculty of Engineering and Information Sciences, UOW. He is the Director of Institute of Cybersecurity and Cryptology, UOW. He has published more than 300 articles in journals and conference proceedings in cryptography and network security. He has served as a program committee member of several international conferences. He was awarded the prestigious Australian Research Council Future Fellowship, in 2009. In 2016, he was awarded the Researcher of the Year from the UOW, for his research excellence and contributions. His work on the creation of short signature schemes has been well cited and it is a part of the IETF draft. He is the Editor-in-Chief of the Information journal.

JOONSANG BAEK received the Ph.D. degree from Monash University, Australia, in 2004. His Ph.D. thesis was on the security analysis of sign-cryption. He has received great attention from the research community. He was a Research Scientist with the Institute for Infocomm Research, Singapore, and an Assistant Professor with the Khalifa University of Science and Technology, United Arab Emirates. He is a Senior Lecturer with the School of Computer Science and Information Technology and a member of the Institute of Cybersecurity and Cryptology, University of Wollongong (UOW), Australia. He has published his work in numerous reputed journals and conference proceedings. His current research interests are in the fields of applied cryptography and cybersecurity. He has also served as a program committee member and the chair of a number of renowned conferences on information security and cryptography.