

Heterogeneous Broadcast Signcryption Scheme With Equality Test for IoVs

Yingzhe Hou¹, Yue Cao², Senior Member, IEEE, Hu Xiong³, Senior Member, IEEE,
Jiawen Kang⁴, Senior Member, IEEE, Chuan Heng Foh⁵, Senior Member, IEEE,
and Changyu Dong, Member, IEEE

Abstract—To ensure the privacy and security of charging services under Internet of Vehicles (IoVs) environment, it is critical to secure the charging stations (CSs) interaction with multiple electric vehicles (EVs). In this paper, we construct a heterogeneous broadcast signcryption protocol supporting equality test for IoVs (HBSC-ET), which addresses the communication problem between a CS and EVs featured with one-to-Many properties. In our design, the CS is allocated in public key infrastructure cryptosystem (PKI), while the EVs are equipped in identity-based cryptography (IBC). In order to address the restriction of EVs storage resources, the received ciphertexts at EV side, are alternatively uploaded to cloud server running equality test. Here, the cloud server legitimately executes the equality test, to determine whether two ciphertexts conclude the same message without unsigncryption. With this, the design HBSC-ET is advanced in terms of information utilization ratio. Finally, the rigorous experiment as well as performance analysis elaborate that our proposed scheme is more suitable for charging services in IoVs.

Index Terms—Broadcast signcryption, equality test, Internet of Vehicles, electric vehicles, heterogeneity.

I. INTRODUCTION

THE rapid development of Internet of vehicles (IoVs) has the possibility to improve the quality of individuals and organizations [1]. With the popularity of Electric Vehicles (EVs) and its environmental friendly benefits for the IoVs in future, the charging service or battery swap service have attracted the attention of researchers [2], [3]. Here, a typical communication

Manuscript received 2 March 2023; revised 17 December 2023 and 11 July 2024; accepted 9 August 2024. Date of publication 14 August 2024; date of current version 19 December 2024. This work was supported by Wuhan Industrial base Innovation Program under Grant 2023010402010783. The review of this article was coordinated by Dr. Tomoaki Ohtsuki. (*Corresponding author: Yue Cao*)

Yingzhe Hou and Yue Cao are with the School of Cyber Science and Engineering, Wuhan University, Wuhan 430000, China (e-mail: hyzpxl@gmail.com; yue.cao@whu.edu.cn).

Hu Xiong is with the School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China (e-mail: xionghu.uestc@gmail.com).

Jiawen Kang is with the School of Automation, Guangdong University of Technology, Guangzhou 510006, China (e-mail: kjwx886@163.com).

Chuan Heng Foh is with the 5G and 6G Innovation Centre, Institute for Communication Systems (ICS), University of Surrey, GU2 7XH Guildford, U.K. (e-mail: c.foh@surrey.ac.uk).

Changyu Dong is with the Institute of AI and Blockchain, Guangzhou University, Guangzhou 511370, China (e-mail: changyu.dong@gmail.com).

Digital Object Identifier 10.1109/TVT.2024.3443103

system enabling the charging service in practice requires the charging station (CS) to disseminate its operation information to EVs using reliable and secure channels. (e.g., 5G with certain level of security mechanism to protect the confidentiality, integrity and unforgeability of information). Nowadays, leading manufacturers, e.g., NIO and Tesla have been already built their own secure operation cycle [4], [5].

Despite the charging service that brings a lot of conveniences for EV users and potential in achieving global trend to promote E-Mobility ecosystem, the security of information exchanged for making charging service decisions is still a critical problem [6]. In order to avoid the information disclosure between CS and EVs particularly under the information dissemination manner with “One-to-Many” feature, the broadcast encryption primitive is introduced accordingly [7]. Based on this idea, the CS is regarded as a broadcast center, to encrypt the information so that the authorized receiver has the ability to restore the ciphertext with the corresponding private key. Meanwhile, the non-authorized receiver cannot restore the information, even if the broadcast information is intercepted inadvertently. Therefore, the introduced protocol ensures the CS (as one broadcaster) distributes broadcast information to large-scale authorized EVs (as multiple receivers) simultaneously, which greatly reduces the cost of previous one-to-one delivery. After this mechanism, numerous schemes originating from broadcast encryption are presented successively [8], [9], [10], [11], [12].

Nevertheless, the broadcast encryption can only guarantee the confidentiality of messages, while the authenticity of messages cannot be preserved. Fortunately, the primitive of signcryption is also considered as a desirable solution to guarantee the confidentiality, unforgeability of messages simultaneously [13], [14], [15]. In this manner, the encryption and signature function are both implemented in a single operation, rather than the traditional signature-then-encryption mode, and this can reduce the computing overhead greatly. Thus, Li et al. [16] established the first broadcast signcryption scheme. In their scheme, the identity-based cryptography (IBC) and broadcast signcryption are merged. The former IBC solves the management problem of certificate during traditional public key infrastructure (PKI), while the latter broadcast signcryption ensures the security requirement. Then, Zhao et al. [17] formulated an efficient broadcast signcryption scheme for platoon communication, which can achieve the same security level with low overhead. Nevertheless, the schemes of [16] and [17] are constructed under a single

and pure IBC system, and thus the communication devices in heterogeneous systems are not applicable apparently.

Since IoVs involve a number of network entities in supporting communications under dynamic and heterogeneous scenario, how to adapt to a heterogeneous environment rather than a single system has been studied in [18]. The heterogeneous signcryption primitive is constructed by Huang et al. [19]. In their scheme, the sender is assigned in the IBC system and the receiver is assigned in the PKI system. Based on [19], two heterogeneous signcryption protocols are proposed in [20]. The first protocol delivers the message from PKI to IBC and the second protocol delivers the message from IBC to PKI. Therefore, the two-way transmission of messages can be guaranteed concurrently. However, a heterogeneous broadcast signcryption towards one-to-many state has not been investigated in the literature.

In IoVs, we can observe that it is infeasible to store a large number of signcryption ciphertext on vehicle itself, due to limited storage and computation capability of vehicle on-board-unit [21]. To address this problem, the device generally chooses to upload the ciphertext to the cloud server, which has access to store and handle the ciphertext with the powerful processing ability [22]. Nonetheless, it suffers from inconvenience in searching ciphertext in terms of signcryption [23]. During the traditional scheme, if one user intends to search the required information from the cloud server, it must download all the stored ciphertext and decrypt them, which results in numerous computational redundancy. Thankfully, the primitive of keyword search is introduced to improve searching efficiency of ciphertext [24]. In this mechanism, the cloud server only can perform the search process with different ciphertexts encrypted by the same public key. Following this, the first equality test scheme is introduced by Yang et al. [25], which can support the equality test under ciphertexts encrypted by the same or different public keys.

Integrating the equality test with the heterogeneous signcryption, Xiong et al. [26] proposed the heterogeneous signcryption scheme supporting equality test. Whereas, above schemes are constructed for “One-to-One” manner that does not support broadcasting communication nature. Considering the above comprehensive reasons, we construct a heterogeneous broadcast signcryption protocol supporting the function of equality test (HBSC-ET). The system model of concrete scene is elaborated in Fig. 1. The CS serves as a broadcaster and signcrypts the condition information to EVs, then the authorized EVs unsigncrypt the ciphertext and obtain the information. Besides, they also can back up the ciphertext to the cloud server for improving the searchability. In this HBSC-ET scheme, the retrieval operation is performed by the cloud server. It only needs to execute the equality test on two ciphertexts from different public key encryption. If the test result is true, which indicates that the retrieval is successful; otherwise, the test result is false, which indicates that the retrieval failed. Finally, the cloud server returns the test results to the required EV, and then EV only needs to decrypt the ciphertext that matches successfully. Therefore, it greatly reduces the retrieval cost and improves the utilization of the ciphertext. The concrete contributions are demonstrated as follows:

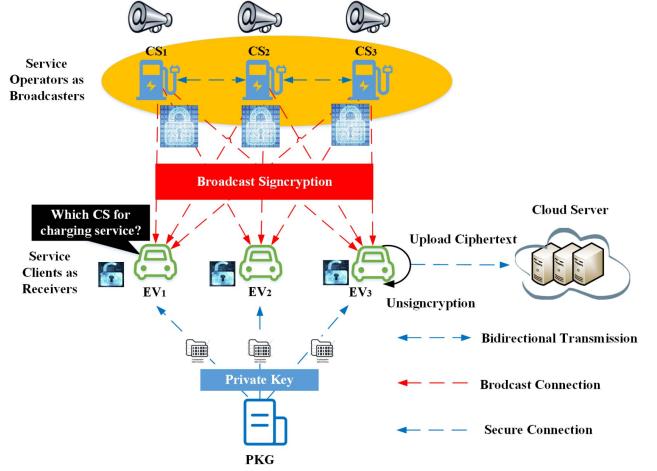


Fig. 1. The charging service system model of HBSC-ET.

- Aiming to the “One-to-Many” communication nature under the E-Mobility service, our HBSC-ET scheme enables CS to distribute the same signcryption information to multiple EVs. By this means, the times of message delivery is diminished by broadcast mechanism and the transmission delay is significantly reduced. Meanwhile, the constant signcrypted ciphertext is generated, and thus the ciphertext redundancy is reduced accordingly.
- The proposed HBSC-ET scheme is based on heterogeneous broadcast signcryption. In this manner, the confidentiality, integrity and unforgeability of message are preserved simultaneously. Besides, the construction is proven to achieve the security of selective indistinguishability chosen plaintext attacks (IND-CPA), one way chosen plaintext attacks (OW-CPA) and existential unforgeability against adaptive chosen messages attacks (EUF-CMA).
- This paper allows the cloud server to execute equality test to facilitate the search of ciphertext signcrypted with the same or different public keys. Compared with the system that does not apply the cloud server for equality testing, this is the advantage of improving the utilization of ciphertext apparently. The analysis of performance elaborates that our HBSC-ET is more suitable for the secure charging services.

II. RELATED WORKS

A. Equality Test

The first public key encryption with equality test (PKEET) protocol is constructed in [25]. During this scheme, anyone can perform the equality test on ciphertexts encrypted by the same or different public keys. Then, Tang [27] proposed the fine-grained authorization scheme (FG-PKEET), via a trusted proxy to authorize two users who possess their own public/private key pairs to perform equality test on ciphertexts. Following this, the all-or-nothing PKEET (AoN-PKEET) is introduced in [28]. This scheme can specify a user to execute the equality test on ciphertext. Furthermore, Tang [29] extended the scheme presented in [27] to a two-agent model, where the agent performs the equality test. Then, a public key encryption with delegated

equality test (PKE-DET) is formulated [30], this scheme enables the delegated organization to execute this operation. Huang et al. [31] introduced a public key encryption supporting authorized equality test (PKE-AET), to allow a receiver to authorize a specific ciphertext. After the development of PKE-AET, numerous schemes based on PKEET are constructed sequentially. Notably, the encryption mechanism only guarantees the confidentiality of message, while the concept of signcryption is introduced to guarantee the confidentiality and authenticity simultaneously. The first heterogeneous signcryption protocol with equality test is demonstrated in [26]. The first heterogeneous signcryption scheme attempting to address the heterogeneous devices problem by supporting equality test is demonstrated in [26]. In a recent work, Xiong et al. [32] also presented a heterogeneous signcryption protocol from IBC to PKI supporting equality test towards wireless body area networks (WBANs).

B. Signcryption

The research based on encryption scheme can guarantee the confidentiality of the message, but cannot guarantee the authenticity [33], [34]. The first signcryption scheme is constructed by Zheng et al. [13], which inherits the advantages of signature and encryption. Inspired by [13], some efficient schemes based on signcryption are published in [15], [35]. Malone-Lee [36] used the bilinear pairings to construct the identity-based signcryption scheme (IBSC), to provide a concrete security model and guarantee the unforgeability and privacy. However, the authors in [37] point out that the message's signature is visible, and the scheme in [37] can not achieve semantic security. Chow et al. [38] then introduced a new identity-based signcryption scheme. In this manner, the forward security and public verifiability are both supported. Their scheme requires two private keys and thus the communication overhead is increased. The scheme in [36] is extended by Boyen [39], in which the unlinkability, authentication and anonymity of ciphertext are added. Finally, Chen and Malone-Lee [40] improved the scheme presented in [39] and constructed a most efficient IBSC protocol.

The above schemes are generally arranged in the same cryptosystem. The real scenario is complex and changeable, the security requirements of the devices involved are different. Thus, the information exchange between different devices belongs to a heterogeneous condition. Huang et al. [19] introduced a new primitive named heterogeneous signcryption, which addresses a practical scenario from an identity-based user to a server with a certificate environment. Subsequently, Pan et al. [41] suggested a heterogeneous signcryption protocol between the unmanned aerial vehicle (UAV) and the ground station (GS), in which the UAV is assigned in IBC environment, while the GS is assigned in PKI environment. Following this, two heterogeneous signcryption protocols are introduced in Li [20], the first message transmission direction is from IBC to PKI, and the second transmission direction is PKI to IBC. The heterogeneous signcryption scheme supporting equality test (HSC-ET) is constructed in [26], in which a sensor in PKI can deliver the message to a user in IBC.

Obviously, the aforesaid schemes are only suitable for the communication manner between one sender and one receiver.

TABLE I
NOTIONS AND SYMBOLS

Notations	Explanation
G_1, G_2	Two multiplicative groups
g	The generator of G_1
u	The element in G_1
p	The prime order of G_1
msk	The master secret key
sp	The system parameter
$H_i (1 \leq i \leq 6)$	The hash function
sk_s	The sender's private key (CS)
pk_s	The sender's public key (CS)
ID_i	The identity of receivers (EVs)
S	The authorization ID_i list
SK_{ID_i}	The private key of receivers (EVs)
td	The receiver's trapdoor
M	The transmission message
C	The broadcast signcryption ciphertext
\perp	The returned result is empty
1	The equality test result is true
0	The equality test result is false
CS	The Charging Station
EV	The Electric Vehicle
PKG	Private Key Generation
$ Z_p^* $	The length of one element in Z_p^*
$ G_1 $	The length of one element in G_1
$ G_2 $	The length of one element in G_2

If there exist multiple receivers in environment, the concept of broadcast signcryption inheriting the advantages of broadcast encryption is advocated to address this challenge [42]. Zhong et al. [43] introduced a broadcast encryption protocol for vehicles communication in IoVs. In this primitive, one sender delivers the information to several receivers, and just the authorized objects could recover the plaintext, while the other users cannot decrypt the ciphertext. Li et al. [16] described the identity-based broadcast signcryption protocol (IBBSC). Through this cryptosystem, the authentication and nonrepudiation defects are resolved currently. However, none of above works apply to the case of distributing the broadcast message in heterogeneous environment from PKI to IBC and guaranteeing the searchability of ciphertext at the same time.

III. PRELIMINARIES

The mathematical background, the definition, the security and system model, the algorithm flow of HBSC-ET are demonstrated as follows. The concrete significance of symbols are showed in Table I.

A. Mathematical Problems and Bilinear Maps

Bilinear Maps: Given two cyclic groups G_1 and G_2 , where the generator and prime order of G_1 are g and p , respectively. Define the bilinear pairing $e : G_1 \times G_1 \rightarrow G_2$ and satisfy the following properties:

- 1) **Bilinearity:** Given $E, I \in G_1$, $a, b \in Z_p^*$, $e(E^a, I^b) = e(E, I)^{ab}$.
 - 2) **Non-degeneracy:** $e(E, I)^{ab} \neq 1$.
- (f, g, F)-General Decisional Diffie-Hellman Exponent problem ((f, g, F)-GDDHEP) [44]: Input $g_0, g_0^{s^2}, \dots, g_0^{s^{k-1}}, g_0^{s \cdot f(h)}, g_0^{\gamma \cdot s \cdot f(s)}, u_0, u_0^s, u_0^{s^2}, \dots, u_0^{s^{2n}}, u_0^{\gamma \cdot g(s)}$, judge $\omega = e(g_0, u_0)^{\gamma \cdot f(s)}$ is the target of \mathcal{C} , where

$\omega, g_0, u_0 \in G_1$, $k, n, s \in Z_p^*$. Besides, the unitary polynomials f and g are described:

$$f(x) = \prod_{i=1}^k (x + x_i)$$

$$g(x) = \prod_{i=k+1}^{k+n} (x + x_i)$$

$$f_i(x) = \frac{f(x)}{x + x_i}, i \in [1, k]$$

$$g_i(x) = \frac{g(x)}{x + x_i}, i \in [k+1, k+n]$$

q -strong Diffie-Hellman Problem (q-SDHP) [20]: Input $(q+1)$ instances $(v, v^a, v^{a^2}, \dots, v^{a^q})$, the target is to find a pair $(y, v^{\frac{1}{a+y}})$, where $y, a \in Z_p^*$.

B. Definitions

Our HBSC-ET scheme includes seven algorithms. The algorithms and their functions are described as follows.

- **Setup**: Input the security parameter k , then PKG outputs msk and the system parameters sp .
- **PKI-KG**: Input sp , then the sender during PKI system generates the private and public key pairs (sk_s, pk_s) .
- **IBC-KG**: Input msk, sp , a group of receivers' identities $S = \{ID_i\}_{i=1}^n$ in IBC system, then PKG generates the corresponding private key SK_{ID_i} .
- **Trapdoor**: Input sp and SK_{ID_i} , and the receiver generates its trapdoor td .
- **Signcrypt**: Input sp , the plaintext M , the sender's private key sk_s , a group of receivers' identities $S = \{ID_i\}_{i=1}^n$, and the sender generates the ciphertext C .
- **UnSigncrypt**: Input sp , the ciphertext C , the sender's public key pk_s and the private key of receiver SK_{ID_i} , the receiver generates M or \perp .
- **Test**: Input two ciphertexts C_α, C_β and the trapdoor td_α, td_β , the cloud server generates the result "1" (which means that the equality test is held, and the compared ciphertexts contain the same message) or "0" (which means that the equality test is not valid, and the compared ciphertexts contain different messages).

C. System Model

The system model is expounded in Fig. 1. There exist four entities which are CS, EV, PKG and Cloud Server.

- 1) **CS**: It refers to the Charging Station, which is considered as a fully-trusted entity. It is allocated in PKI system and delivered the transmitted information to required EVs.
- 2) **EV**: It is named the Electric Vehicle, which requires to obtain the charging information from CS. It is allocated in IBC system and divided into two types. If EV belongs to an authorized group receiver, such as $ID_i \in \{0, 1, \dots, n\}$, it have the access to decrypt the ciphertext and get the real

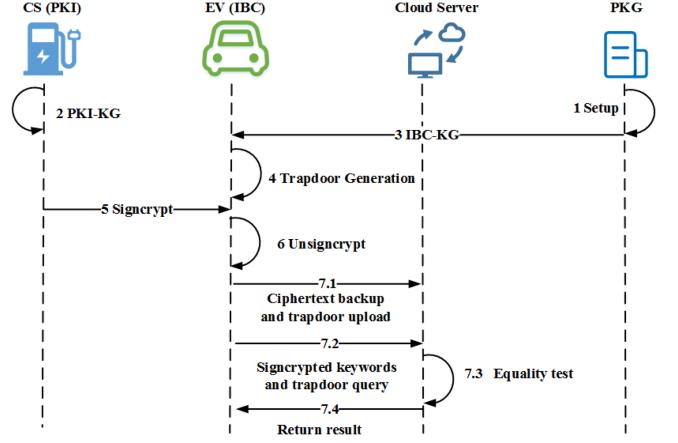


Fig. 2. The algorithm flow of HBSC-ET in IoVs.

information. If it does not belong to an authorized group receiver, it will try its best to attack the authorized user to get more information.

- 3) **PKG**: It refers to the Private Key Generation, which is also considered as a fully-trusted entity, it is employed to generate the private key of each EV.
- 4) **Cloud Server**: This entity is a semi-trusted third party, which is utilized to perform the equality test and return the outcome to the corresponding EV.

Algorithm Flow: The algorithm flow of HBSC-ET is illustrated in Fig. 2 and the flow is explained as follows in steps. (1) The PKG performs the Setup step and outputs sp, msk to CS and EVs; (2) The CS performs the PKI-KG operation to output the public and private key pair; (3) The PKG performs the IBC-KG operation and generates the private key to required EVs; (4) The EVs performs the trapdoor generation operation to output the corresponding trapdoor; (5) The CS in PKI executes the signcryption step to generate the ciphertext C ; (6) After receiving the ciphertext, the EVs in IBC executes the unsigncryption step to recover the plaintext M ; (7) The EVs can upload the ciphertext and trapdoor to cloud server; (8) When an EV intends to query some message, it will upload the signcrypted keywords and its trapdoor to cloud server; (9) The cloud server performs the equality test operation on ciphertext encrypted by the same or different public keys; (10) Finally, the cloud server returns the equality test's result to the corresponding EV.

D. Security Models

Definition 1: Assuming that there is no adversary \mathcal{A}_1 wins this game with a non-negligible advantage, the HBSC-ET scheme can achieve the IND-CPA secure.

Game 1. We define a challenger \mathcal{C} and an adversary \mathcal{A}_1 , they interact with each other as well as execute operations as below.

- **Initial**: The $I^* = \{ID_1^*, ID_2^*, \dots, ID_m^*\}$ is set as the challenge list by \mathcal{A}_1 .
- **Setup**: The **Setup** operation is executed by \mathcal{C} . Then the system parameters sp , the private and public key of sender (sk_s^*, pk_s^*) are delivered to \mathcal{A}_1 .
- **Phase 1**: \mathcal{A}_1 adaptively executes queries as below:

- Private key query: when this query is issued, \mathcal{C} executes IBC-KG operation and delivers SK_{ID_r} to \mathcal{A}_1 .
- *Challenge*: \mathcal{A}_1 picks two same length messages M_0^* , M_1^* and regards ID_r^* as the challenge. \mathcal{C} will choose $\rho \in \{0, 1\}$. Besides, the challenge ciphertext is delivered from \mathcal{C} to \mathcal{A}_1 .
- *Phase 2*: This operation is the same as *Phase 1*. The restriction is that the private key of ID_i cannot be asked, in which $ID_i \in I^*$.
- *Guess*: \mathcal{A}_1 generates ρ' . \mathcal{A}_1 wins if $\rho' = \rho$.

Definition 2: Assuming that there is no adversary \mathcal{A}_2 wins this game with a non-negligible advantage, the HBSC-ET scheme can achieve the OW-CPA secure.

Game 2 . We define a challenger \mathcal{C} and an adversary \mathcal{A}_2 , they interact with each other and execute operations as below.

- *Initial*: The $I^* = \{ID_1^*, ID_2^*, \dots, ID_{m^*}^*\}$ is set as the challenge list by \mathcal{A}_2 .
- *Setup*: The *Setup* operation is executed by \mathcal{C} . Then the system parameters sp , the public key of sender pk_s^* are delivered to \mathcal{A}_2 .
- *Phase 1*: \mathcal{A}_2 adaptively executes queries as below:
 - Private key query: when this query is issued, \mathcal{C} executes IBC-KG operation and delivers SK_{ID_i} to \mathcal{A}_2 .
 - Trapdoor query: when this query is issued, \mathcal{C} executes the Private key query and delivers $SK_{ID_{i,2}}$ to \mathcal{A}_2 .
- *Challenge*: \mathcal{A}_2 picks the plaintext M^* and ID_r^* as the challenge identity. Then, the challenge ciphertext is delivered from \mathcal{C} to \mathcal{A}_2 .
- *Phase 2*: This operation is the same as *Phase 1*. The restriction is that the private key of ID_i cannot be asked, in which $ID_i \in I^*$.
- *Guess*: \mathcal{A}_2 generates M' . \mathcal{A}_2 wins if $M' = M^*$.

Definition 3: Assuming that there is no adversary \mathcal{A}_3 wins this game with a non-negligible advantage, the HBSC-ET scheme can achieve the EUF-CMA secure.

Game 3 . We define a challenger \mathcal{C} and an adversary \mathcal{A}_3 , they interact with each other and execute operations as below.

- *Setup*: The *Setup* operation is executed by \mathcal{C} . Then the system parameters sp , the master secret key msk , the public key of sender pk_s^* are delivered to \mathcal{A}_3 .
- *Phase 1*: \mathcal{A}_3 adaptively executes queries as below:
 - Private key query: when this query is issued, \mathcal{C} delivers SK_{ID_r} and sk_s to \mathcal{A}_3 .
 - Signcryption query: when this query is issued with M , the sender's private key sk_s , the identity lists $\{ID_r\}_{r=1}^n$, \mathcal{C} executes the *Signcrypt* operation and delivers C to \mathcal{A}_3 .
- *Forgery*: \mathcal{A}_3 produces the identity of receiver ID_r^* , the new ciphertext C^* . If the result of $Unsigncrypt(C^*, pk_s^*, SK_{ID_r^*})$ is not \perp , that is to say, \mathcal{A}_3 wins this game.

IV. CONSTRUCTION

In this section, we elaborate the detailed construction as below.

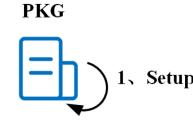


Fig. 3. The system model of Setup.

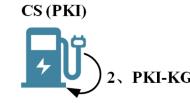


Fig. 4. The system model of PKI Key Generation.

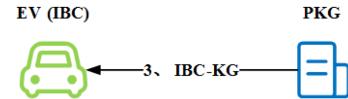


Fig. 5. The system model of IBC Key Generation.

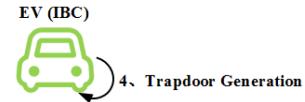


Fig. 6. The system model of Trapdoor Generation.

- 1) *Setup*: Define two cyclic groups G_1 and G_2 , where the prime order and the generator of G_1 are p and g , the bilinear map is described as $e : G_1 \times G_1 \rightarrow G_2$. After receiving the security parameter k , PKG selects $s_1, s_2 \in Z_p^*$, $u \in G$, and computes $t = e(g, u)$. Then it calculates $g_1 = g^{s_1}$, $g_2 = g^{s_2}$, $u^{s_1}, u^{s_1^2}, \dots, u^{s_1^n}$, $u^{s_2}, u^{s_2^2}, \dots, u^{s_2^n}$, in which n represents the number of vehicles receiving broadcast messages. Choose six hash functions, $H_1 : \{0, 1\}^* \rightarrow Z_p^*$, $H_2 : \{0, 1\}^* \rightarrow Z_p^*$, $H_3 : G_2 \rightarrow \{0, 1\}^*$, $H_4 : \{0, 1\}^n \rightarrow Z_p^*$, $H_5 : G_2 \rightarrow Z_p^*$, $H_6 : \{0, 1\}^n \times G_2 \times G_2 \times \{0, 1\}^* \times Z_p^* \rightarrow Z_p^*$. Besides, $msk = (s_1, s_2)$ is defined as the master secret key. The system public parameter is $sp = (G_1, G_2, q, g_1, g_2, u, t, u^{s_1}, u^{s_1^2}, \dots, u^{s_1^n}, u^{s_2}, u^{s_2^2}, \dots, u^{s_2^n}, e, H_1, H_2, H_3, H_4, H_5, H_6)$. The corresponding system model is shown in Fig. 3.
- 2) *PKI-KG*: After receiving sp , the sender in PKI system randomly picks $x_s \in Z_p^*$, then it computes the private key $sk_s = g^{\frac{1}{x_s}}$, the public key $pk_s = u^{x_s}$. The system model of this step is elaborated in Fig. 4.
- 3) *IBC-KG*: After receiving sp , a group of receivers' identities $S = \{ID_i\}_{i=1}^n$ in IBC system, PKG computes the private key $SK_{ID_i} = (SK_{ID_{i,1}}, SK_{ID_{i,2}})$, where $SK_{ID_{i,1}} = g^{\frac{1}{s_1+H_1(ID_i)}}, SK_{ID_{i,2}} = g^{\frac{1}{s_2+H_2(ID_i)}}$. The system model of this step is elaborated in Fig. 5.
- 4) *Trapdoor*: Given the private key SK_{ID_i} , the receiver generates $td = SK_{ID_{i,2}}$ as the trapdoor. The system model of this step is elaborated in Fig. 6.
- 5) *Signcrypt*: Given the message M , the private key of sender sk_s , a group of receivers' identities $S = \{ID_i\}_{i=1}^n$, the system model of this step is elaborated in Fig. 7. The sender picks $\gamma_1, \gamma_2 \in Z_p^*$ and calculates

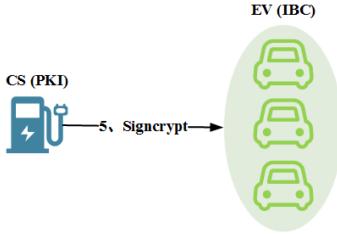


Fig. 7. The system model of generate ciphertext.

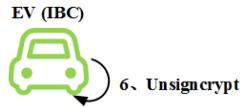


Fig. 8. The system model of unsigncrypt ciphertext.

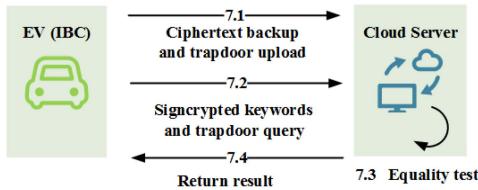


Fig. 9. The system model of equality test.

- $\Gamma_1 = t^{\gamma_1}$, $\Gamma_2 = t^{\gamma_2}$.
- $C_1 = (M||\gamma_2) \oplus H_3(\Gamma_1)$.
- $C_2 = (\gamma_2 \cdot H_4(M)) \oplus H_5(\Gamma_2)$.
- $f = H_6(M, \Gamma_1, \Gamma_2, C_1, C_2)$.
- $C_3 = g_1^{-\gamma_1}$, $C_4 = g_2^{-\gamma_2}$.
- $C_5 = sk_s^{(\gamma_1+f)}$.
- $C_6 = u^{\gamma_1} \prod_{i=1}^n (s_1 + H_1(ID_i))$.
- $C_7 = u^{\gamma_2} \prod_{i=1}^n (s_2 + H_2(ID_i))$.
- Generate the ciphertext $C = (C_1, C_2, C_3, C_4, C_5, C_6, C_7)$.
- 6) UnSigncrypt: Given sp , the ciphertext C , and the public key of sender pk_s . The identity of receiver ID_i with its private key $SK_{ID_i} = (SK_{ID_{i,1}}, SK_{ID_{i,2}})$ calculates the following operations, where $ID_i \in S$.
 - $\Gamma_1 = [e(C_3, u^{\Delta_{s_1}}) \cdot e(SK_{ID_{i,1}}, C_6)] \prod_{i=1, i \neq r}^n H_1(ID_i)$.
 - $\Gamma_2 = [e(C_4, u^{\Delta_{s_2}}) \cdot e(SK_{ID_{i,2}}, C_7)] \prod_{i=1, i \neq r}^n H_2(ID_i)$.
 - $\Delta_{s_1} = \frac{1}{s_1} (\prod_{i=1, i \neq r}^n (s_1 + H_1(ID_i)) - \prod_{i=1, i \neq r}^n H_1(ID_i))$.
 - $\Delta_{s_2} = \frac{1}{s_2} (\prod_{i=1, i \neq r}^n (s_2 + H_2(ID_i)) - \prod_{i=1, i \neq r}^n H_2(ID_i))$.
 - $M||\gamma_2 = C_1 \oplus H_3(\Gamma_1)$.
 - $f' = H_6(M, \Gamma_1, \Gamma_2, C_1, C_2)$.
 - Check whether $C_2 \oplus (\gamma_2 \cdot H_4(M)) \stackrel{?}{=} H_5(\Gamma_2)$, $e(C_5, pk_s) t^{-f'} \stackrel{?}{=} \Gamma_1$. The system model is elaborated in Fig. 8.
- 7) Test: Given two ciphertexts $C_\alpha = (C_{\alpha,1}, C_{\alpha,2}, C_{\alpha,3}, C_{\alpha,4}, C_{\alpha,5}, C_{\alpha,6}, C_{\alpha,7})$, $C_\beta = (C_{\beta,1}, C_{\beta,2}, C_{\beta,3}, C_{\beta,4}, C_{\beta,5}, C_{\beta,6}, C_{\beta,7})$, two trapdoor td_α, td_β , the cloud server executes the following operations. This system model is elaborated in Fig. 9.
 - $\Gamma_{\alpha,2} = [e(C_{\alpha,4}, u^{\Delta_{s_2}}) \cdot e(td_\alpha, C_{\alpha,7})] \prod_{i=1, i \neq r}^n H_1(ID_i)$.

- $\Gamma_{\beta,2} = [e(C_{\beta,4}, u^{\Delta_{s_2}}) \cdot e(td_\beta, C_{\beta,7})] \prod_{i=1, i \neq r}^n H_2(ID_i)$.
- $\gamma_{\alpha,2} \cdot H_4(M_\alpha) = C_{\alpha,2} \oplus H_5(\Gamma_{\alpha,2})$.
- $\gamma_{\beta,2} \cdot H_4(M_\beta) = C_{\beta,2} \oplus H_5(\Gamma_{\beta,2})$.
- Check $\Gamma_{\alpha,2}^{\gamma_{\beta,2} \cdot H_4(M_\beta)} = \Gamma_{\beta,2}^{\gamma_{\alpha,2} \cdot H_4(M_\alpha)}$.

Correctness:

$$\begin{aligned}
 \Gamma_1 &= [e(C_3, u^{\Delta_{s_1}}) \cdot e(SK_{ID_{i,1}}, C_6)] \prod_{i=1, i \neq r}^n H_1(ID_i) \\
 &= [e(g, u)^{-\gamma_1} (\prod_{i=1, i \neq r}^n (s_1 + H_1(ID_i)) - \prod_{i=1, i \neq r}^n H_1(ID_i))] \\
 &\quad \cdot e(g, u)^{\gamma_1} (\prod_{i=1, i \neq r}^n (s_1 + H_1(ID_i))] \prod_{i=1, i \neq r}^n H_1(ID_i) \\
 &= [e(g, u)^{\gamma_1} \prod_{i=1, i \neq r}^n H_1(ID_i)] \prod_{i=1, i \neq r}^n H_1(ID_i) \\
 &= e(g, u)^{\gamma_1} \\
 &= t^{\gamma_1} \\
 \Gamma_2 &= [e(C_4, u^{\Delta_{s_2}}) \cdot e(SK_{ID_{i,2}}, C_7)] \prod_{i=1, i \neq r}^n H_2(ID_i) \\
 &= [e(g, u)^{-\gamma_2} (\prod_{i=1, i \neq r}^n (s_2 + H_2(ID_i)) - \prod_{i=1, i \neq r}^n H_2(ID_i))] \\
 &\quad \cdot e(g, u)^{\gamma_2} (\prod_{i=1, i \neq r}^n (s_2 + H_2(ID_i))] \prod_{i=1, i \neq r}^n H_2(ID_i) \\
 &= [e(g, u)^{\gamma_2} \prod_{i=1, i \neq r}^n H_2(ID_i)] \prod_{i=1, i \neq r}^n H_2(ID_i) \\
 &= e(g, u)^{\gamma_2} \\
 &= t^{\gamma_2} \\
 e(C_5, pk_s) t^{-f'} &= e(sk_s^{(\gamma_1+f)}, pk_s) t^{-f'} \\
 &= e(g^{\frac{1}{x_s}(\gamma_1+f)}, u^{x_s}) t^{-f'} \\
 &= e(g, u)^{(\gamma_1+f)} t^{-f'} \\
 &= t^{(\gamma_1+f)} t^{-f'} \\
 &= t^{\gamma_1} \\
 &= \Gamma_1 \\
 \Gamma_{\alpha,2}^{\gamma_{\beta,2} \cdot H_4(M_\beta)} &= t^{\gamma_{\alpha,2} \gamma_{\beta,2} \cdot H_4(M_\beta)} \\
 \Gamma_{\beta,2}^{\gamma_{\alpha,2} \cdot H_4(M_\alpha)} &= t^{\gamma_{\beta,2} \gamma_{\alpha,2} \cdot H_4(M_\alpha)}
 \end{aligned}$$

V. SECURITY ANALYSIS

Theorem 1: If the adversary \mathcal{A}_1 can break the HBSC-ET scheme with advantage ε , there exists a challenger \mathcal{C} that can solve the (f, g, F) -GDDHEP with advantage $\varepsilon' = \frac{1}{2}\varepsilon$, the formulated scheme HBSC-ET will reach the security of IND-CPA.

Proof: Given the following instance, \mathcal{A}_1 interacts with \mathcal{C} to conduct this game.

$$\begin{aligned}
 &g_0, g_0^s, g_0^{s^2}, \dots, g_0^{s^{k-1}}, g_0^{s \cdot f(h)}, g_0^{\gamma \cdot s \cdot f(s)} \\
 &u_0, u_0^s, u_0^{s^2}, \dots, u_0^{s^{2n}}, u_0^{\gamma \cdot g(s)}
 \end{aligned}$$

The target of \mathcal{C} is to decide $\omega = e(g_0, u_0)^{\gamma \cdot f(s)}$, where $\omega \in G_2$, the number of queries of \mathcal{A}_1 is k , the input of \mathcal{C} and \mathcal{A}_1 is n .

Besides, the unitary polynomials f and g is set:

$$\begin{aligned} f(x) &= \prod_{i=1}^k (x + x_i) \\ g(x) &= \prod_{i=k+1}^{k+n} (x + x_i) \\ f_i(x) &= \frac{f(x)}{x + x_i}, i \in [1, k] \\ g_i(x) &= \frac{g(x)}{x + x_i}, i \in [k+1, k+n] \end{aligned}$$

Initial: Set $I^* = \{ID_1^*, ID_2^*, \dots, ID_{m^*}^*\}$ as the challenge list, in which $m^* \leq n$.

Setup: \mathcal{C} sets $g = g_0^{f(s)}$, picks $\zeta_1, \zeta_2 \in Z_p^*$, and computes $s_1 = \zeta_1 \cdot s, s_2 = \zeta_2 \cdot s, g_1 = g_0^{s_1 \cdot f(s)} = g^{s_1}, g_2 = g_0^{s_2 \cdot f(s)} = g^{s_2}, u = \prod_{i=k+m^*+1}^{k+n} (s_1 + x_i) = u_0^{\prod_{i=k+m^*+1}^{k+n} (s_2 + y_i)}$. Therefore, we can obtain

$$\begin{aligned} t &= e(g_0, u_0)^{f(s) \cdot \prod_{i=k+m^*+1}^{k+n} (s_1 + x_i)} \\ &= e(g_0, u_0)^{f(s) \cdot \prod_{i=k+m^*+1}^{k+n} (s_2 + y_i)} \\ &= e(g, u) \end{aligned}$$

Finally, \mathcal{C} sends the $sp = (G_1, G_2, q, g_1, g_2, u, t, u^s, u^{s^2}, \dots, u^{s^n}, u^{s^2}, u^{s^2}, \dots, u^{s^n}, e, H_1, H_2, H_3, H_4, H_5, H_6)$, the private and public key of sender (sk_s^*, pk_s^*) to \mathcal{A}_1 .

Phase 1: The six initial empty lists $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3, \mathcal{L}_4, \mathcal{L}_5, \mathcal{L}_6$ are maintained by \mathcal{C} , which are employed to simulate the oracles. The challenge identity of receiver ID_r^* is delivered to H_1 at some point. Besides, other query on ID_r is based on H_1 query.

- H_1 query: After receiving the identity ID_i , \mathcal{C} first searches the item $(ID_i, x_i, SK_{ID_{i,1}})$ from \mathcal{L}_1 . If it exists, \mathcal{C} delivers x_i to \mathcal{A}_1 . Otherwise, \mathcal{C} chooses $x_i \in Z_p^*$, then inserts $(ID_i, x_i, *)$ into \mathcal{L}_1 . Finally, \mathcal{C} delivers x_i to \mathcal{A}_1 .
- H_2 query: After receiving the identity ID_i , \mathcal{C} first searches the item $(ID_i, y_i, SK_{ID_{i,2}})$ from \mathcal{L}_2 . If it exists, \mathcal{C} delivers y_i to \mathcal{A}_1 . Otherwise, \mathcal{C} chooses $y_i \in Z_p^*$, then inserts $(ID_i, y_i, *)$ into \mathcal{L}_2 . Finally, \mathcal{C} delivers y_i to \mathcal{A}_1 .
- H_3 query: When obtaining this query, \mathcal{C} searches the item (Γ_1, h_3) from \mathcal{L}_3 . If it exists, \mathcal{C} delivers h_3 to \mathcal{A}_1 . Otherwise, \mathcal{C} chooses $h_3 \in \{0, 1\}^*$, then inserts (Γ_1, h_3) into \mathcal{L}_3 . Finally, \mathcal{C} delivers h_3 to \mathcal{A}_1 .
- H_4 query: When obtaining this query, \mathcal{C} searches the item (M, h_4) from \mathcal{L}_4 . If it exists, \mathcal{C} delivers h_4 to \mathcal{A}_1 . Otherwise, \mathcal{C} chooses $h_4 \in Z_p^*$, then inserts (M, h_4) into \mathcal{L}_4 . Finally, \mathcal{C} delivers h_4 to \mathcal{A}_1 .
- H_5 query: When obtaining this query, \mathcal{C} searches the item (Γ_2, h_5) from \mathcal{L}_5 . If it exists, \mathcal{C} delivers h_5 to \mathcal{A}_1 . Otherwise, \mathcal{C} chooses $h_5 \in Z_p^*$, then inserts (Γ_2, h_5) into \mathcal{L}_5 . Finally, \mathcal{C} delivers h_5 to \mathcal{A}_1 .
- H_6 query: When obtaining this query, \mathcal{C} searches the item $(M, \Gamma_1, \Gamma_2, C_1, C_2)$ from \mathcal{L}_6 . If it exists, \mathcal{C} delivers h_6 to \mathcal{A}_1 . Otherwise, \mathcal{C} chooses $h_6 \in Z_p^*$, then inserts

$(M, \Gamma_1, \Gamma_2, C_1, C_2, h_6)$ into \mathcal{L}_6 . Finally, \mathcal{C} delivers h_6 to \mathcal{A}_1 .

- Private key query: When obtaining this query with ID_i . If $ID_i = ID_r^*$, \mathcal{C} aborts. Otherwise, \mathcal{C} searches $(ID_i, x_i, SK_{ID_{i,1}}), (ID_i, y_i, SK_{ID_{i,2}})$ from $\mathcal{L}_1, \mathcal{L}_2$ and delivers $SK_{ID_i} = (SK_{ID_{i,1}}, SK_{ID_{i,2}})$ to \mathcal{A}_1 . Else, \mathcal{C} computes

$$\begin{aligned} SK_{ID_{i,1}} &= g^{\frac{1}{s_1 + H_1(ID_i)}} \\ SK_{ID_{i,2}} &= g^{\frac{1}{s_2 + H_2(ID_i)}} \end{aligned}$$

Then, \mathcal{C} updates $(ID_i, x_i, SK_{ID_{i,1}}), (ID_i, y_i, SK_{ID_{i,2}})$ and delivers SK_{ID_i} to \mathcal{A}_1 .

- Trapdoor query: When obtaining this query, if $ID_i = ID_r^*$, \mathcal{C} aborts; Otherwise, \mathcal{C} searches \mathcal{L}_2 and delivers $td = SK_{ID_{i,2}}$ to \mathcal{A}_1 .

Challenge: After finished the above-mentioned queries, if $ID_i \neq ID_r^*$, \mathcal{C} aborts. Otherwise, \mathcal{C} performs the **Signcrypt** step, \mathcal{C} picks $\gamma_1, \gamma_2 \in Z_p^*$ and computes

$$\begin{aligned} C_1^* &= (M || \gamma_2) \oplus H_3(\Gamma_1) \\ C_2^* &= (\gamma_2 \cdot H_4(M)) \oplus H_5(\Gamma_2) \\ C_3^* &= g_0^{-\gamma_1 \cdot s_1 \cdot f(s)} \\ C_4^* &= g_0^{-\gamma_2 \cdot s_2 \cdot f(s)} \\ C_5^* &\in G_1 \\ C_6^* &= u_0^{\gamma_1 \cdot g(s)} \\ C_7^* &= u_0^{\gamma_2 \cdot g(s)} \end{aligned}$$

where

$$\begin{aligned} \Gamma_1 &= \Omega^{\prod_{i=k+m^*+1}^{k+n} x_i} \cdot e(g_0^{\gamma_1 \cdot s_1 \cdot f(s)}, u_0^{\Delta_{s_1}}), \\ \Gamma_2 &= \Omega^{\prod_{i=k+m^*+1}^{k+n} y_i} \cdot e(g_0^{\gamma_2 \cdot s_2 \cdot f(s)}, u_0^{\Delta_{s_2}}), \\ \Delta_{s_1} &= \frac{1}{s_1} \left(\prod_{i=k+m^*+1}^{k+n} (s_1 + H_1(ID_i)) - \prod_{i=k+m^*+1}^{k+n} H_1(ID_i) \right), \\ \Delta_{s_2} &= \frac{1}{s_2} \left(\prod_{i=k+m^*+1}^{k+n} (s_2 + H_2(ID_i)) - \prod_{i=k+m^*+1}^{k+n} H_2(ID_i) \right), \end{aligned}$$

Finally, \mathcal{C} delivers $C^* = (C_1^*, C_2^*, C_3^*, C_4^*, C_5^*, C_6^*, C_7^*)$ as the challenge ciphertext to \mathcal{A}_1 . The following equations are verified:

$$\begin{aligned} C_3^* &= g_1^{-\gamma_1} \\ C_4^* &= g_2^{-\gamma_2} \\ C_6^* &= u^{\gamma_1 \prod_{i=k+m^*+1}^{k+n} (s_1 + x_i) \cdot \prod_{i=k+1}^{k+m^*} (s_1 + x_i)} \\ &= u_0^{\prod_{i=k+1}^{k+m^*} (s_1 + H_1(ID_i))} \\ C_7^* &= u_0^{\gamma_2 \prod_{i=k+m^*+1}^{k+n} (s_2 + y_i) \cdot \prod_{i=k+1}^{k+m^*} (s_2 + y_i)} \\ &= u_0^{\prod_{i=k+1}^{k+m^*} (s_2 + H_2(ID_i))} \end{aligned}$$

Suppose if $\gamma_1 = \zeta_1 \cdot \gamma$, $\gamma_2 = \zeta_2 \cdot \gamma$, $\omega = e(g_0, u_0)^{\gamma \cdot f(s)}$, we can obtain

$$\begin{aligned}\omega_1 &= e(g_0, u_0)^{\gamma_1 \cdot f(s)} = e(g_0, u_0)^{\zeta_1 \cdot \gamma \cdot f(s)} = \omega^{\zeta_1} \\ \omega_2 &= e(g_0, u_0)^{\gamma_2 \cdot f(s)} = e(g_0, u_0)^{\zeta_2 \cdot \gamma \cdot f(s)} = \omega^{\zeta_2}\end{aligned}$$

and thus the equations $\Gamma_1 = t^{\gamma_1}$, $\Gamma_2 = t^{\gamma_2}$ are held. The correctness is demonstrated as follows:

$$\begin{aligned}\Gamma_1 &= \omega_1^{\prod_{i=k+m^*+1}^{k+n} x_i} \cdot e(g_0^{\gamma_1 \cdot s_1 \cdot f(s)}, u_0^{\Delta_{s_1}}) \\ &= e(g_0, u_0)^{\gamma_1 \cdot f(s) \cdot \prod_{i=k+m^*+1}^{k+n} x_i} \cdot e(g_0^{\gamma_1 \cdot s_1 \cdot f(s)}, u_0^{\Delta_{s_1}}) \\ &= e(g_0, u_0)^{\gamma_1 \cdot f(s) \cdot \prod_{i=k+m^*+1}^{k+n} x_i} \\ &\quad \cdot e(g_0^{\gamma_1 \cdot s_1 \cdot f(s)}, u_0^{\frac{1}{s_1}(\prod_{i=k+m^*+1}^{k+n} (s_1+x_i) - \prod_{i=k+m^*+1}^{k+n} x_i)}) \\ &= e(g_0, u_0)^{\gamma_1 \cdot f(s) \cdot \prod_{i=k+m^*+1}^{k+n} x_i} \\ &\quad \cdot e(g_0, u_0)^{\gamma_1 \cdot f(s)(\prod_{i=k+m^*+1}^{k+n} (s_1+x_i) - \prod_{i=k+m^*+1}^{k+n} x_i)} \\ &= e(g_0, u_0)^{\gamma_1 \cdot f(s) \cdot \prod_{i=k+m^*+1}^{k+n} (s_1+x_i)} \\ &= e(g_0^f(s), u_0^{\prod_{i=k+m^*+1}^{k+n} (s_1+x_i)})^{\gamma_1} \\ &= e(g, u)^{\gamma_1} \\ &= t^{\gamma_1} \\ \Gamma_2 &= \omega_2^{\prod_{i=k+m^*+1}^{k+n} y_i} \cdot e(g_0^{\gamma_2 \cdot s_2 \cdot f(s)}, u_0^{\Delta_{s_2}}) \\ &= e(g_0, u_0)^{\gamma_2 \cdot f(s) \cdot \prod_{i=k+m^*+1}^{k+n} y_i} \cdot e(g_0^{\gamma_2 \cdot s_2 \cdot f(s)}, u_0^{\Delta_{s_2}}) \\ &= e(g_0, u_0)^{\gamma_2 \cdot f(s) \cdot \prod_{i=k+m^*+1}^{k+n} y_i} \\ &\quad \cdot e(g_0^{\gamma_2 \cdot s_2 \cdot f(s)}, u_0^{\frac{1}{s_2}(\prod_{i=k+m^*+1}^{k+n} (s_2+y_i) - \prod_{i=k+m^*+1}^{k+n} y_i)}) \\ &= e(g_0, u_0)^{\gamma_2 \cdot f(s) \cdot \prod_{i=k+m^*+1}^{k+n} y_i} \\ &\quad \cdot e(g_0, u_0)^{\gamma_2 \cdot f(s)(\prod_{i=k+m^*+1}^{k+n} (s_2+y_i) - \prod_{i=k+m^*+1}^{k+n} y_i)} \\ &= e(g_0, u_0)^{\gamma_2 \cdot f(s) \cdot \prod_{i=k+m^*+1}^{k+n} (s_2+y_i)} \\ &= e(g_0^f(s), u_0^{\prod_{i=k+m^*+1}^{k+n} (s_2+y_i)})^{\gamma_2} \\ &= e(g, u)^{\gamma_2} \\ &= t^{\gamma_2}\end{aligned}$$

\mathcal{C} chooses $\rho \in \{0, 1\}$, defines $\Gamma_\rho = \Gamma_1$ and computes $M_\rho || \gamma_2 = C_1^* \oplus H_3(\Gamma_\rho)$.

Phase 2: In this section, \mathcal{A}_1 makes the same query as *Phase 1*. Nonetheless, the restriction is $ID_i \notin I^*$.

Guess: \mathcal{A}_1 generates ρ' , if $\rho' = \rho$, we say that \mathcal{A}_1 wins this game.

Analysis: Thus, we can obtain

$$\begin{aligned}\varepsilon' &= \Pr[\rho' = \rho | \text{real}] - \Pr[\rho' = \rho | \text{rand}] \\ &= \frac{1}{2} \times (\Pr[\rho' = 1 | \rho = 1 \wedge \text{real}] - \Pr[\rho' = 1 | \rho = 0 \wedge \text{real}])\end{aligned}$$

$$\begin{aligned}&- \frac{1}{2} \times (\Pr[\rho' = 1 | \rho = 1 \wedge \text{rand}] \\ &\quad - \Pr[\rho' = 1 | \rho = 0 \wedge \text{rand}])\end{aligned}$$

In the random oracle $[\text{rand}]$, as respect to the adversary view, the distribution of ρ is independent. Therefore,

$$\Pr[\rho' = 1 | \rho = 1 \wedge \text{rand}] = \Pr[\rho' = 1 | \rho = 0 \wedge \text{rand}].$$

In the real environment $[\text{real}]$, the emulations executed by \mathcal{C} are perfect due to their constructions satisfy the semantic security game. Therefore,

$$\varepsilon = \Pr[\rho' = 1 | \rho = 1 \wedge \text{real}] - \Pr[\rho' = 1 | \rho = 0 \wedge \text{real}].$$

According to the above equations, we can get $\varepsilon' = \frac{1}{2}\varepsilon$.

Theorem 2: If the adversary \mathcal{A}_2 can against HBSC-ET with the advantage ε , there exists \mathcal{C} can solve the (f, g, F) -GDDHEP with advantage $\varepsilon' = \frac{1}{2} - \frac{\varepsilon}{2^n}$, the formulated scheme HBSC-ET will reach the security of OW-CPA.

Proof: Given the following instance, \mathcal{A}_2 interacts with \mathcal{C} to conduct this section.

$$\begin{aligned}g_0, g_0^s, g_0^{s^2}, \dots, g_0^{s^{k-1}}, g_0^{s \cdot f(h)}, g_0^{\gamma \cdot s \cdot f(s)} \\ u_0, u_0^s, u_0^{s^2}, \dots, u_0^{s^{2n}}, u_0^{\gamma \cdot g(s)}\end{aligned}$$

The target of \mathcal{C} is to decide $\omega = e(g_0, u_0)^{\gamma \cdot f(s)}$, where $\omega \in G_2$, the number query of \mathcal{A}_2 is k , the input of \mathcal{C} and \mathcal{A}_2 is n . Besides, the unitary polynomials f and g is set:

$$\begin{aligned}f(x) &= \prod_{i=1}^k (x + x_i) \\ g(x) &= \prod_{i=k+1}^{k+n} (x + x_i) \\ f_i(x) &= \frac{f(x)}{x + x_i}, i \in [1, k] \\ g_i(x) &= \frac{g(x)}{x + x_i}, i \in [k+1, k+n]\end{aligned}$$

Initial: Set $I^* = \{ID_1^*, ID_2^*, \dots, ID_{m^*}^*\}$ as the challenge list, where $m^* \leq n$.

Setup: \mathcal{C} sets $g = g_0^{f(s)}$, picks $\zeta_1 \in Z_p^*$, and computes $s_1 = \zeta_1 \cdot s$, $g_1 = g_0^{s_1 \cdot f(s)} = g^{s_1}$, $u = u_0^{\prod_{i=k+m^*+1}^{k+n} (s_1+x_i)}$. Therefore, we can obtain

$$\begin{aligned}t &= e(g_0, u_0)^{f(s) \cdot \prod_{i=k+m^*+1}^{k+n} (s_1+x_i)} \\ &= e(g, u)\end{aligned}$$

Finally, \mathcal{C} sends the $sp = (G_1, G_2, q, g_1, g_2, u, t, u^s, u^{s^2}, \dots, u^{s^n}, u^{s_2}, \dots, u^{s_2^n}, e, H_1, H_2, H_3, H_4, H_5, H_6)$, the private and public key of sender (sk_s^*, pk_s^*) to \mathcal{A}_2 .

Phase 1: The six initial empty lists $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3, \mathcal{L}_4, \mathcal{L}_5, \mathcal{L}_6$ are maintained by \mathcal{C} , which are employed to simulate the oracles.

- H_i query ($1 \leq i \leq 6$): These queries are the similar as Theorem 1 except H_2 query.

- H_2 query: When obtaining the identity ID_i , \mathcal{C} searches the item $(ID_i, y_i, SK_{ID_{i,2}})$ from \mathcal{L}_2 . If it exists, \mathcal{C} delivers y_i to \mathcal{A}_2 . Otherwise, \mathcal{C} chooses $y_i \in Z_p^*$, calculates $SK_{ID_{i,2}} = g^{\frac{1}{s_2+y_i}}$, then inserts $(ID_i, y_i, SK_{ID_{i,2}})$ into \mathcal{L}_2 . Finally, \mathcal{C} delivers y_i to \mathcal{A}_2 .
- Private key query: When obtaining this query with ID_i . If $ID_i = ID_r^*$, \mathcal{C} aborts. Otherwise, \mathcal{C} searches $(ID_i, x_i, SK_{ID_{i,1}})$, $(ID_i, y_i, SK_{ID_{i,2}})$ from \mathcal{L}_1 , \mathcal{L}_2 , and delivers $SK_{ID_i} = (SK_{ID_{i,1}}, SK_{ID_{i,2}})$ to \mathcal{A}_2 . Else, \mathcal{C} computes

$$SK_{ID_{i,1}} = g^{\frac{1}{s_1+H_1(ID_i)}}$$

Then, \mathcal{C} updates $(ID_i, x_i, SK_{ID_{i,1}})$ in \mathcal{L}_1 and delivers $SK_{ID_i} = (SK_{ID_{i,1}}, SK_{ID_{i,2}})$ to \mathcal{A}_2 .

- Trapdoor query: When obtaining this query, \mathcal{C} searches \mathcal{L}_2 and delivers $td = SK_{ID_{i,2}}$ to \mathcal{A}_2 .

Challenge: After finished the above-mentioned queries, if $ID_i \neq ID_r^*$, \mathcal{C} aborts. Otherwise, \mathcal{C} performs the `Signcrypt` step, \mathcal{C} picks $\gamma_1, \gamma_2 \in Z_p^*$ and chooses $C_2^* \in Z_p^*, C_4^*, C_5^*, C_7^* \in G_1$. Then \mathcal{C} computes

$$\begin{aligned} C_1^* &= (M||\gamma_2) \oplus H_3(\Gamma_1) \\ C_3^* &= g_0^{-\gamma_1 \cdot s_1 \cdot f(s)} \\ C_6^* &= u_0^{\gamma_1 \cdot g(s)} \end{aligned}$$

where

$$\begin{aligned} \Gamma_1 &= \Omega^{\prod_{i=k+m^*+1}^{k+n} x_i} \cdot e(g_0^{\gamma_1 \cdot s_1 \cdot f(s)}, u_0^{\Delta_{s_1}}) \\ \Delta_{s_1} &= \frac{1}{s_1} \left(\prod_{i=k+m^*+1}^{k+n} (s_1 + H_1(ID_i)) - \prod_{i=k+m^*+1}^{k+n} H_1(ID_i) \right) \end{aligned}$$

Finally, \mathcal{C} delivers the challenge ciphertext $C^* = (C_1^*, C_2^*, C_3^*, C_4^*, C_5^*, C_6^*, C_7^*)$ to \mathcal{A}_2 . The following equations are verified:

$$\begin{aligned} C_3^* &= g_1^{-\gamma_1} \\ C_6^* &= u^{\gamma_1 \cdot \prod_{i=k+m^*+1}^{k+n} (s_1+x_i) \cdot \prod_{i=k+1}^{k+m^*} (s_1+x_i)} \\ &= u_0^{\prod_{i=k+1}^{k+m^*} (s_1+H_1(ID_i^*))} \end{aligned}$$

If $\gamma_1 = \zeta_1 \cdot \gamma$, $\omega = e(g_0, u_0)^{\gamma \cdot f(s)}$, we can obtain

$$\omega_1 = e(g_0, u_0)^{\gamma_1 \cdot f(s)} = e(g_0, u_0)^{\zeta_1 \cdot \gamma \cdot f(s)} = \omega^{\zeta_1}$$

and thus the equation $\Gamma_1 = t^{\gamma_1}$ is held. The correctness is demonstrated as follows:

$$\begin{aligned} \Gamma_1 &= \omega_1^{\prod_{i=k+m^*+1}^{k+n} x_i} \cdot e(g_0^{\gamma_1 \cdot s_1 \cdot f(s)}, u_0^{\Delta_{s_1}}) \\ &= e(g_0, u_0)^{\gamma_1 \cdot f(s) \cdot \prod_{i=k+m^*+1}^{k+n} x_i} \cdot e(g_0^{\gamma_1 \cdot s_1 \cdot f(s)}, u_0^{\Delta_{s_1}}) \\ &= e(g_0, u_0)^{\gamma_1 \cdot f(s) \cdot \prod_{i=k+m^*+1}^{k+n} x_i} \\ &\quad \cdot e(g_0^{\gamma_1 \cdot s_1 \cdot f(s)}, u_0^{\frac{1}{s_1} (\prod_{i=k+m^*+1}^{k+n} (s_1+x_i) - \prod_{i=k+m^*+1}^{k+n} x_i)}) \\ &= e(g_0, u_0)^{\gamma_1 \cdot f(s) \cdot \prod_{i=k+m^*+1}^{k+n} x_i} \end{aligned}$$

$$\begin{aligned} &\cdot e(g_0, u_0)^{\gamma_1 \cdot f(s) (\prod_{i=k+m^*+1}^{k+n} (s_1+x_i) - \prod_{i=k+m^*+1}^{k+n} x_i)} \\ &= e(g_0, u_0)^{\gamma_1 \cdot f(s) \cdot \prod_{i=k+m^*+1}^{k+n} (s_1+x_i)} \\ &= e(g_0^{\gamma_1 \cdot f(s)}, u_0^{\prod_{i=k+m^*+1}^{k+n} (s_1+x_i)})^{\gamma_1} \\ &= e(g, u)^{\gamma_1} \\ &= t^{\gamma_1} \end{aligned}$$

\mathcal{C} chooses $M^* \in \{0, 1\}^n$, defines $\Gamma_{M^*} = \Gamma_1$ and computes $M^*||\gamma_2 = C_1^* \oplus H_3(\Gamma_{M^*})$.

Phase 2: In this section, \mathcal{A}_2 makes the same query as *Phase 1*. Nonetheless, the constraint is $ID_i \notin I^*$.

Guess: \mathcal{A}_2 generates M' , if $M' = M^*$, we say that \mathcal{A}_2 wins this game.

Analysis: From the aforementioned game, we can obtain

$$\varepsilon' = \Pr[M' = M^* | \text{real}] - \Pr[M' = M^* | \text{rand}]$$

In the random oracle `[rand]`, since $M^* \in \{0, 1\}^n$, and thus, \mathcal{A}_2 has the ability of $\frac{1}{2^n} \times \varepsilon$ to guess $M' = M^*$.

In the real environment `[real]`, \mathcal{A}_2 has the ability of $\frac{1}{2}$ to guess $M' = M^*$.

According to the above analyses, we can compute $\varepsilon' = \frac{1}{2} - \frac{\varepsilon}{2^n}$.

Theorem 3: If the adversary \mathcal{A}_3 can against HBSC-ET with the advantage ε , there has \mathcal{C} can solve the q-SDHP with advantage $\varepsilon' \geq \frac{\varepsilon}{q}$, the proposed scheme will achieve EUF-CMA security.

Proof: Given $(v, v^a, v^{a^2}, \dots, v^{a^q})$, the challenger \mathcal{C} interacts with adversary \mathcal{A}_3 to find a pair $(y, v^{\frac{1}{a+y}})$, where $y \in Z_p^*$.

Setup: \mathcal{C} chooses $\tau^*, \tau_1, \tau_2, \dots, \tau_{q-1} \in Z_p^*$ and the polynomial is expanded as follows:

$$f(\kappa) = \prod_{i=1}^{q-1} (\kappa + \tau_i) = \sum_{j=0}^{q-1} r_j \kappa^j.$$

Then, we define that

$$\begin{aligned} g &= v^{\sum_{j=0}^{q-1} r_j a^j} = v^{f(a)} \\ g_1 &= v^{\sum_{j=1}^q r_{j-1} a^j} = v^{af(a)} = g^a \\ f_i(\kappa) &= \frac{f(\kappa)}{\kappa + \tau_i} + \sum_{j=0}^{q-2} p_j \kappa^j \end{aligned}$$

and thus \mathcal{C} can compute

$$Q_i = v^{\sum_{j=0}^{q-2} p_j \kappa^j} = v_i^{f(a)} = v_i^{\frac{f(a)}{a+\tau_i}} = g^{\frac{1}{a+\tau_i}}.$$

Finally, \mathcal{C} can access the pairs $(\tau_i, Q_i = g^{\frac{1}{a+\tau_i}})$. \mathcal{C} chooses $u^a, u^{a^2}, \dots, u^{a^t} \in Z_p^*$ and computes $t = e(g, u)$. Then, the system parameter is $sp = (G_1, G_2, q, g_1, g_2, u, t, u^a, u^{a^2}, \dots, u^{a^t}, u^{s_2}, u^{s_2^2}, \dots, u^{s_2^t}, e, H_1, H_2, H_3, H_4, H_5, H_6)$, the master secret key is $msk = (g, s_1, s_2)$ and delivered to \mathcal{A}_3 . The six initial empty lists $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3, \mathcal{L}_4, \mathcal{L}_5, \mathcal{L}_6$ are maintained by \mathcal{C} . Besides, \mathcal{C} delivers the public key of sender $pk_s^* = u^{a+\tau^*}$ to \mathcal{A}_3 , where $a = s_1$.

Queries: In this section, \mathcal{A}_3 makes the following queries:

- H_1 query: After receiving the identity ID_i , \mathcal{C} first searches that if \mathcal{L}_1 contains ID_i . If it exists, \mathcal{C} delivers $H_1(ID_i) = I_i$ to \mathcal{A}_3 . Else, \mathcal{C} chooses $I_i \in Z_p^*$ and inserts (ID_i, I_i) into \mathcal{L}_1 . Finally, \mathcal{C} delivers I_i to \mathcal{A}_3 .
- H_2 query: After receiving the identity ID_i , \mathcal{C} first searches the item (ID_i, h_2) from \mathcal{L}_2 . If it exists, \mathcal{C} delivers h_2 to \mathcal{A}_3 . Otherwise, \mathcal{C} chooses $h_2 \in Z_p^*$, then inserts (ID_i, h_2) into \mathcal{L}_2 . Finally, \mathcal{C} delivers h_2 to \mathcal{A}_3 .
- H_3 query: After receiving this query, \mathcal{C} first searches the item (Γ_1, h_3) from \mathcal{L}_3 . If it exists, \mathcal{C} delivers h_3 to \mathcal{A}_3 . Otherwise, \mathcal{C} chooses $h_3 \in \{0, 1\}^*$, then inserts (Γ_1, h_3) into \mathcal{L}_3 . Finally, \mathcal{C} delivers h_3 to \mathcal{A}_3 .
- H_4 query: After receiving this query, \mathcal{C} first searches the item (M, h_4) from \mathcal{L}_4 . If it exists, \mathcal{C} delivers h_4 to \mathcal{A}_3 . Otherwise, \mathcal{C} chooses $h_4 \in Z_p^*$, then inserts (M, h_4) into \mathcal{L}_4 . Finally, \mathcal{C} delivers h_4 to \mathcal{A}_3 .
- H_5 query: After receiving this query, \mathcal{C} first searches the item (Γ_2, h_5) from \mathcal{L}_5 . If it exists, \mathcal{C} delivers h_5 to \mathcal{A}_3 . Otherwise, \mathcal{C} chooses $h_5 \in Z_p^*$, then inserts (Γ_2, h_5) into \mathcal{L}_5 . Finally, \mathcal{C} delivers h_5 to \mathcal{A}_3 .
- H_6 query: After receiving this query, \mathcal{C} first searches the item $(M, \Gamma_1, \Gamma_2, C_1, C_2)$ from \mathcal{L}_6 . If it exists, \mathcal{C} delivers h_6 to \mathcal{A}_3 . Otherwise, \mathcal{C} chooses $h_6 \in Z_p^*$, then inserts $(M, \Gamma_1, \Gamma_2, C_1, C_2, h_6)$ into \mathcal{L}_6 . Then, \mathcal{C} sends h_6 to \mathcal{A}_3 .
- Private key query: After receiving this query on sender. \mathcal{C} picks $I_s \in Z_p^*$ and computes $sk_s = g^{\frac{1}{s_1+I_s}}$ as the private key of sender. Towards the challenge sender, \mathcal{C} picks $I_s^* \in Z_p^*$ and computes $sk_s^* = g^{\frac{1}{a+I_s^*}}$, in which $I_s^* = \tau^*$. However, \mathcal{C} keeps sk_s^* and cannot deliver to \mathcal{A}_3 . When receiving this query on the identity of receiver ID_j , \mathcal{C} will compute $Q_j = g^{\frac{1}{s_1+I_j}}$ to \mathcal{A}_3 . Please obtain that in this section, \mathcal{A}_3 has the knowledge msk and obtains all the private key of receiver.
- Signcryption query: At any moment, \mathcal{A}_3 could execute the signcryption query with the message M and the identity of receiver ID_j . \mathcal{C} obtains the receiver's private key $SK_{ID_j} = (SK_{ID_{j,1}}, SK_{ID_{j,2}}) = (Q_j, g^{\frac{1}{s_2+h_2}})$. Then \mathcal{C} performs the following operations:
 - 1) Pick $x, \gamma_1, \gamma_2, f \in Z_p^*$.
 - 2) Compute $C_3 = (g_1 g^{I_j})^f g_1^{-x}$.
 - 3) Compute $C_4 = g_2^{-\gamma_2}$.
 - 4) Compute $C_5 = SK_{ID_{j,1}}^x$.
 - 5) Compute $C_6 = u^{\gamma_1 \prod_{j=1}^n (s_1 + I_j)}$.
 - 6) Compute $C_7 = u^{\gamma_2 \prod_{j=1}^n (s_2 + h_2)}$.
 - 7) Compute $\Gamma_1 = [e(C_3 g^{-I_s x}, u^{\Delta_{s_1}}) \cdot e(SK_{ID_{j,1}},$
 $C_6)]^{\frac{1}{\prod_{j=1, j \neq r}^n I_j}}$, in which $\Delta_{s_1} = \frac{1}{s_1+I_j} (\prod_{j=1, j \neq r}^n s_1 + I_j) - \prod_{j=1, j \neq r}^n I_j$.
 - 8) Compute $\Gamma_2 = [e(C_4, u^{\Delta_{s_2}}) \cdot e(SK_{ID_{j,2}},$
 $C_7)]^{\frac{1}{\prod_{i=1, i \neq r}^n h_2}}$, in which $\Delta_{s_2} = \frac{1}{s_2} (\prod_{j=1, j \neq r}^n s_2 + h_2) - \prod_{j=1, j \neq r}^n h_2$.
 - 9) patch the hash function $H_6(M, \Gamma_1, \Gamma_2, C_1, C_2)$ to f . If H_6 is already set, \mathcal{C} fails.
 - 10) Compute $C_1 = (M || \gamma_2) \oplus H_3(\Gamma_1), C_2 = (\gamma_2 \cdot H_4(M)) \oplus H_5(\Gamma_2)$.

Finally, \mathcal{C} delivers $C = (C_1, C_2, C_3, C_4, C_5, C_6, C_7)$ to \mathcal{A}_3 . In this manner, \mathcal{C} sets $\gamma_1 = (\frac{s_1+I_s}{s_1+I_j})x - f$. Therefore, we can pass the verification $e(C_5, pk_s)t^{-f} = \Gamma_1$.

$$C_5 = SK_{ID_{j,1}}^x = (g^{\frac{1}{s_1+I_j}})^{(\gamma_1+f) \cdot \frac{s_1+I_j}{s_1+I_s}} = sk_s^{(\gamma_1+f)}$$

$$e(C_5, pk_s)t^{-f} = e(SK_{ID_{j,1}}^x, pk_s)t^{-f}$$

$$= e(g^{\frac{\gamma_1+f}{s_1+I_s}}, u^{a+I_s})t^{-f}$$

$$= e(g^{\frac{\gamma_1+f}{s_1+I_s}}, u^{s_1+I_s})t^{-f}$$

$$= t^{(\gamma_1+f)}t^{-f} = t^{\gamma_1} = \Gamma_1$$

$$\begin{aligned} \Gamma_1 &= [e(C_3 g^{-I_s x}, u^{\Delta_{s_1}}) \cdot e(SK_{ID_{j,1}}, C_6)]^{\frac{1}{\prod_{j=1, j \neq r}^n I_j}} \\ &= [e(C_3 g_1^{-x} g^{-I_s x}, u^{\frac{1}{s_1+I_j} (\prod_{j=1, j \neq r}^n (s_1 + I_j) - \prod_{j=1, j \neq r}^n I_j)}) \\ &\quad \cdot e(g^{\frac{1}{s_1+I_j}}, u^{\gamma_1 \prod_{j=1}^n (s_1 + I_j)})]^{\frac{1}{\prod_{j=1, j \neq r}^n I_j}} \\ &= [e(g^{-\gamma_1 (s_1 + I_j)}, u^{\frac{1}{s_1+I_j} (\prod_{j=1, j \neq r}^n (s_1 + I_j) - \prod_{j=1, j \neq r}^n I_j)}) \\ &\quad \cdot e(g, u)^{\gamma_1 \prod_{j=1, j \neq r}^n (s_1 + I_j)}]^{\frac{1}{\prod_{j=1, j \neq r}^n I_j}} \\ &= [e(g, u)^{\gamma_1 \prod_{j=1, j \neq r}^n I_j}]^{\frac{1}{\prod_{j=1, j \neq r}^n I_j}} \\ &= t^{\gamma_1} \end{aligned}$$

$$\begin{aligned} \Gamma_2 &= [e(C_4, u^{\Delta_{s_2}}) \cdot e(SK_{ID_{j,2}}, C_7)]^{\frac{1}{\prod_{i=1, i \neq r}^n h_2}} \\ &= [e(g, u)^{-\gamma_2 (\prod_{j=1, j \neq r}^n (s_2 + h_2) - \prod_{j=1, j \neq r}^n h_2)} \\ &\quad \cdot e(g, u)^{\gamma_2 (\prod_{j=1, j \neq r}^n (s_2 + h_2))}]^{\frac{1}{\prod_{j=1, j \neq r}^n h_2}} \\ &= [e(g, u)^{\gamma_2 \prod_{j=1, j \neq r}^n h_2}]^{\frac{1}{\prod_{j=1, j \neq r}^n h_2}} \\ &= e(g, u)^{\gamma_2} \\ &= t^{\gamma_2} \end{aligned}$$

Forgery: According to the forking lemma, if $ID_s \neq ID_s^*$, \mathcal{C} aborts. Else, \mathcal{C} can forge two signed ciphertexts on ID_s^* via the polynomial responds of \mathcal{A}_3 , such as $(\Gamma_1, \Gamma_2, C_1, C_2, C_3, C_4, C_5, C_6, C_7, M^*, f, \gamma_1)$ and $(\Gamma_1, \Gamma_2, C_1, C_2, C_3, C_4, C'_5, C_6, C_7, M^*, f', \gamma_1)$, where $f = H_6(M^*, \Gamma_1, \Gamma_2, C_1, C_2)$, $f' = H_6(M^*, \Gamma_1, \Gamma_2, C_1, C_2)$, $f \neq f'$. Hence, we have

$$e(C_5, pk_s^*)t^{-f} = e(C'_5, pk_s^*)t^{-f'}$$

Thus,

$$e(C_5, pk_s^*)e(g, u)^{-f} = e(C'_5, pk_s^*)e(g, u)^{-f'}$$

$$e(C_5 - C'_5, pk_s^*) = e(g, u)^{f-f'}$$

$$e((C_5 - C'_5)^{(f-f')^{-1}}, pk_s^*) = e(g, u)$$

Since $pk_s^* = u^{a+\tau^*}$, and thus

$$Z^* = (C_5 - C'_5)^{(f-f')^{-1}} = g^{\frac{1}{a+\tau^*}}$$

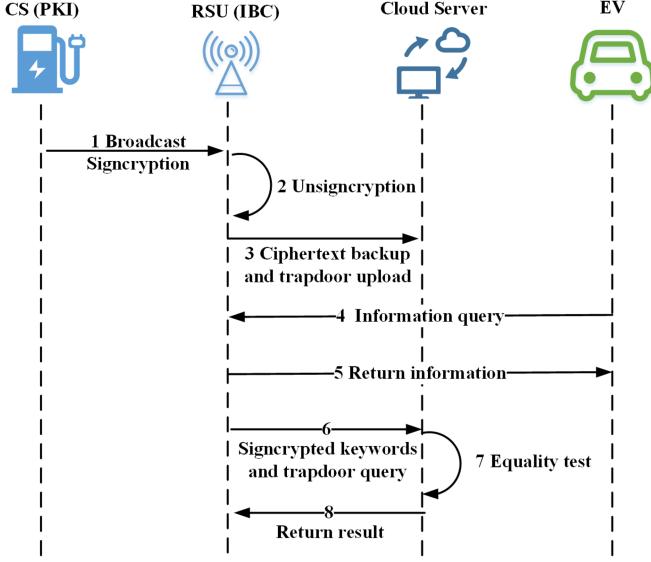


Fig. 10. The algorithm flow of HBSC-ET in [45].

$$\frac{f(a)}{a + \tau^*} = \frac{c}{a + \tau^*} + \sum_{j=0}^{q-2} c_j a^j$$

Therefore,

$$v^{\frac{1}{a+\tau^*}} = \left(\frac{Z^*}{v^{\sum_{j=0}^{q-2} c_j a^j}} \right)^{\frac{1}{c}}$$

C can obtain the pair $(\tau^*, v^{\frac{1}{a+\tau^*}})$, which is the solution of q-SDHP.

Analysis: We define $\Pr[\neg Aborts] = \frac{1}{q}$, where q represents the forgery times of \mathcal{A}_3 . Therefore, the advantage of challenger C to solve q-SDHP is $\epsilon' \geq \frac{\epsilon}{q}$.

Framework analysis: Based on the scheme [45], the publication/services structure is described in Fig. 10. Comparing Figs. 2 and 10, we can observe that HBSC-ET is designed specifically for broadcasting CSs' information exchange, where EVs passively receive encryption information to support its charging service decision made locally. We herein illustrate another paradigm where the charging decision making relies on EVs to proactively trigger CSs information under a point-to-point communication mode. In latter case, the Road Side Unit (RSU) will further oversee the EVs service requests and make charging service. In case there is single failure on RSU service, the charging service will be unavailable for all EVs. In summary, the proposed HBSC-ET decouples the vulnerability of charging decision and security verification, deemed as much reliable system. Of course, the advantage of broadcasting over that publish/subcribe system with infrastructure as assistance, is that ensures the security of information exchange while improving its efficiency. The proposed HBSC-ET is more inclined to enhance the secure transmission and belongs to a heterogeneous broadcast mechanism, while the scheme in [45] pays more attention to the actual efficiency of transmission and belongs to a single system unicast.

TABLE II
THE EXECUTION COST OF CRYPTOGRAPHIC OPERATIONS

Explanation	Symbols	Time
The bilinear pairing operation	T_p	0.5417
The hash to G_1 operation	T_g	2.2039
The exponentiation on G_1 operation	E_1	0.9670
The exponentiation on G_2 operation	E_2	0.0901

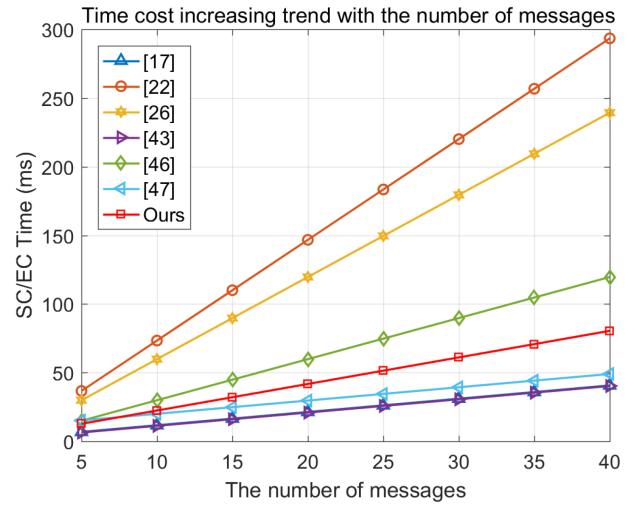


Fig. 11. SC/EC overhead.

VI. PERFORMANCE ANALYSIS

In this section, the comparison between the introduced scheme, the most efficient identity-based broadcast signcryption scheme [17], the identity-based encryption with outsourced equality test solution [22], the first heterogeneous signcryption with equality test protocol [26], the existing broadcast encryption scheme [43], the identity-based signcryption protocol [46], and the certificateless broadcast signcryption scheme supporting equality test [47] in terms of efficiency and security properties are demonstrated. For evaluating the computation overhead of our solution and the schemes based on bilinear pairing, we employ the Pairing Based Cryptography (PBC) library to quantify the concrete time of cryptographic operations. In order to achieve 1024-bit Rivest-Shamir-Adleman (RSA) security, the supersingular curve $E/F_p : y^2 = x^3 + x$ is matched, where 2 is the embedding degree, $q = 2^{159} + 2^{17} + 1$ refers to the 160-bit Solinas prime and $p = 12qr - 1$ is the 512-bit prime. Through the repeated simulation experiments, the running time of cryptographic operations and the corresponding meanings are described in Table II. In addition, the size of $|Z_p^*|$ is 20 bytes and $|G_1| = |G_2|$ is 128 bytes. The features of different protocols are summarized in Table III, in which the symbol “✓” represents satisfied and “✗” indicates not satisfied. From the observation of Table III, the proposed scheme can satisfy all the listed function requirements with efficient performance.

A. Computation Overhead

The computation overhead of competitive schemes is listed in Table IV. Fig. 11 refers to the signcryption or encryption

TABLE III
COMPARISON THE FUNCTIONALITY OF COMPETITIVE SCHEMES

Scheme	CF	UF	AE	Broadcast	Signcryption	Heterogeneous	Equality Test	Security Assumption
Zhao [17]	✓	✓	✓	✓	✓	✗	✗	(f, g, F) -GDDHEP& q-SDHP
Ma [22]	✓	✗	✓	✗	✗	✗	✓	BDHP
Xiong [26]	✓	✓	✓	✗	✓	✓	✓	BDHIP&CDHIP
Zhong [43]	✓	✗	✓	✓	✗	✗	✗	CDHP
Karati [46]	✓	✓	✓	✗	✓	✗	✗	DMBDHIP& MBSDHP
Niu [47]	✓	✓	✗	✓	✓	✗	✓	DDHP& BDHP& CDHP& DBDHP
Our scheme	✓	✓	✓	✓	✓	✓	✓	(f, g, F) -GDDHEP&q-SDHP

* Legends: CF: Confidentiality, UF: Unforgeability, AE: Asymmetric Encryption, BDHP: Bilinear Diffie-Hellman problem, BDHIP: Bilinear Diffie-Hellman Inversion Problem, CDHIP: Computational Diffie-Hellman Inversion Problem, CDHP: Computational Diffie-Hellman, DMBDHIP: Decisional Modified Bilinear Diffie-Hellman Inversion Problem, MBSDHP: Modified Bilinear Strong Diffie-Hellman Problem.

TABLE IV
COMPARISON THE COMPUTATION OVERHEAD OF COMPETITIVE SCHEMES

Protocol	Encryption or Signcryption overhead	Decryption or Unsigncryption overhead	Equality Test overhead
BSPC [17]	$(n+2)E_1+E_2$	$(n+1)E_1+2E_2+3T_p$	—
IBEET [22]	$n(4E_1+2E_2+T_g+2T_p)$	$n(4E_1+T_g+2T_p)$	$2E_1+2T_g+4T_p$
HSCET [26]	$n(6E_1+2E_2)$	$n(E_1+E_2+3T_p)$	$4E_2+4T_p$
IBBE [43]	$(n+1)E_1+E_2+T_p$	$(n-1)E_1+E_2+2T_p$	—
IBSC [46]	$n(3E_1+E_2)$	$n(2E_1+E_2+2T_p)$	—
CLBSC [47]	$(n+6)E_1+2E_2+T_g+4T_p$	$(n+3)E_1+2T_g+2T_p$	E_2+T_p
Our scheme	$(2n+3)E_1+2E_2$	$(2n-2)E_1+3E_2+5T_p$	$4E_2+4T_p$

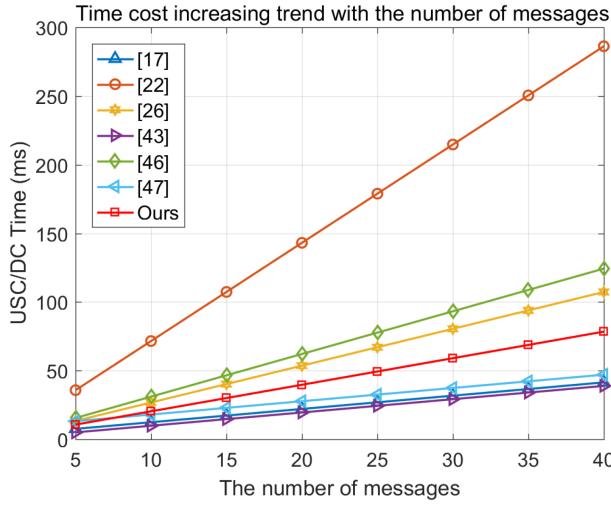


Fig. 12. USC/DC overhead.

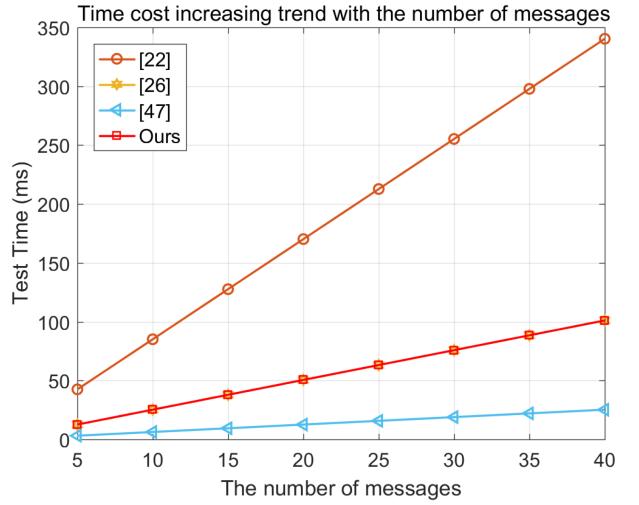


Fig. 13. Test overhead.

cost with the increased number of messages. For example, in scheme [17], $(n+2)$ exponentiations on G_1 and one exponentiation on G_2 are required in signcryption phase. Therefore, the computation overhead of [17] is $(n+2)E_1 + E_2 = 0.9670n + 2.0241\text{ms}$. We can discover that our protocol is more efficient than [22], [26], [46]. In addition, Fig. 12 is the trend of unsigncryption or decryption overhead. There exist $(n+1)$ exponentiations on G_1 , two exponentiations on G_2 and three bilinear pairs during the unsigncryption step of scheme [17]. The unsigncryption speed of our construction is slightly lower than [17], [43], [47]. Furthermore, the time cost of equality test is demonstrated in Fig. 13. Our scheme has a smaller overhead supporting the equality test than [22] and the same overhead as [26].

B. Communication Overhead

Table V and Fig. 14 describe the communication overhead of competitive schemes, we can observe that the schemes based on broadcast mechanism keep the length of the ciphertext unchanged, such as [17], [43], [47] and our protocol. This enables the transmission of multiple messages to maintain a constant communication overhead, to reduce the overall cost tremendously. While, the communication cost in schemes [22], [26], [46] increases with the number of messages increases, it does not apply to lightweight equipment requirements. Besides, the communication overhead of proposed protocol is slightly expensive than [17], [43], [47]. It is forgivable since our solution supports heterogeneous broadcast encryption

TABLE V
COMPARISON THE COMMUNICATION COST OF COMPETITIVE PROTOCOLS

Protocol	The size of ciphertext $ CL $	The size of private key $ SK $	The size of trapdoor $ TD $
Zhao [17]	$4 G_1 + G_2 + Z_p^* $	$ G_1 $	—
Ma [22]	$n(5 G_1 + Z_p^*)$	$2 G_1 $	$ G_1 $
Xiong [26]	$n(4 G_1 + 2 Z_p^*)$	$2 G_1 $	$ G_1 $
Zhong [43]	$2 G_1 + G_2 $	$2 G_1 $	—
Karati [46]	$n(2 G_1 + 2 G_2 + Z_p^*)$	$2 G_1 $	—
Niu [47]	$4 G_1 + 2 G_2 + Z_p^* $	$2 Z_p^* $	$ Z_p^* $
Our scheme	$6 G_1 + 2 Z_p^* $	$2 G_1 $	$ G_1 $

* Legends: we set $|G_1| = |G_2|$.

TABLE VI
COMPARISON WITH AND WITHOUT PROPOSED SCHEME IN CHARGING SERVICE

The number of EVs	The Average Waiting Time Overhead For Switch (s)		Total Switched Batteries (n)	
	No Delay	Delay	No Delay	Delay
200 EVs	426.4	407.9	809	813
300 EVs	1106.3	1141.7	1134	1135
500 EVs	3857.9	4115.2	1257	1260

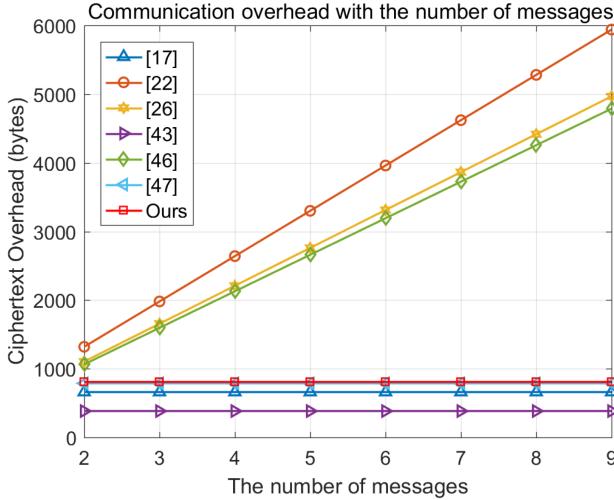


Fig. 14. Communication overhead.

with equality test operation, while the other schemes cannot conform to all these functions.

C. Experimental Analysis

We simulate the charging services experiment in ONE environment with proposed scheme, the underlying charging service is based on our previous work [45], by estimating the service availability of CS and then broadcasting to EVs. Considering security aspect, we have added on the delay at CS and EVs into the service system. The comparison result is elaborated in Table VI. The average waiting time for switch refers to the average period between the EVs arriving at the selected CS time and the battery switch completion time, which is the performance metric of EVs. The intuitive description is shown in Fig. 15. The total switched batteries are employed to describe the total number of EVs that have been switched with batteries at CSs, which is the performance metric of CSs. The corresponding comparison result is shown in Fig. 16. We divide the experiment into three

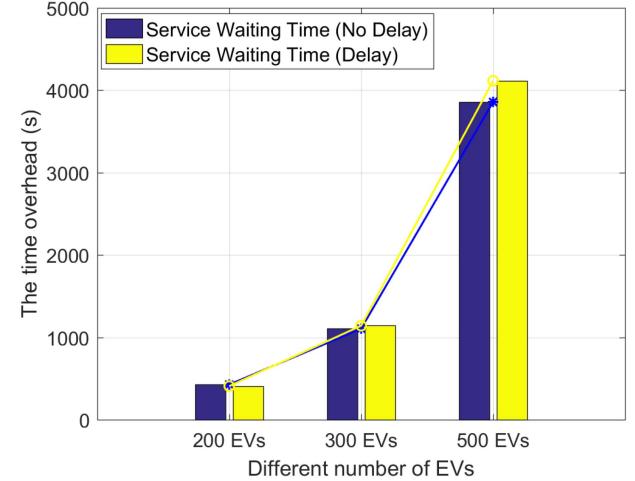


Fig. 15. The comparison of average waiting time for switch.

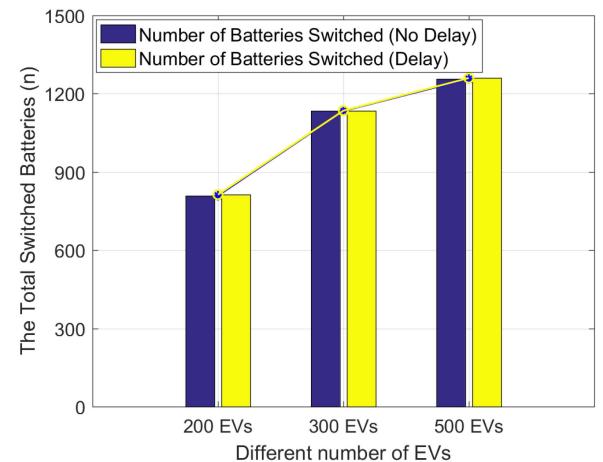


Fig. 16. The comparison of total switched batteries.

groups: 200EVs, 300EVs and 500EVs, respectively. According to Fig. 15, it is evidently to find that towards the average waiting time in 200EVs, the consumption time with delay is shorter

than that without delay. As for the other comparison groups, the cost of delay is slightly higher than those without delay, but the difference is small. Besides, the total switched batteries are almost the same times with the delay or not from Fig. 16. In summary, we demonstrate that the constructed heterogeneous broadcast signcryption protocol is able to secure the system without degrading the application performance.

VII. CONCLUSION

This paper proposed a heterogeneous broadcast signcryption scheme with equality test for IoVs, to provide a feasible solution for heterogeneous mechanisms between PKI and IBC via the broadcast mechanism. By using broadcasting, the same message is employed to send to multiple recipients simultaneously, which greatly reduces the time of message transmissions and improves the efficiency. The cloud server can perform the equality test and determine whether different signcrypted ciphertexts have the same message. Subsequently, the proposed construction is proven to achieve the security of IND-CPA, OW-CPA and EUF-CMA. The performance analysis demonstrated that HBSC-ET is feasible for IoVs. If the private key of a sender is compromised, all message signcryption participated by that sender will no longer be secure. The future work will consider the application of parallel key-insulated heterogeneous signcryption scheme towards IoVs, which updates the private key at different periods and reduces the key disclosure threat during the transmission process greatly.

REFERENCES

- [1] J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao, and C. Liu, “Routing in Internet of Vehicles: A review,” *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 5, pp. 2339–2352, Oct. 2015.
- [2] S. Huang, L. He, Y. Gu, K. Wood, and S. Benjaafar, “Design of a mobile charging service for electric vehicles in an urban environment,” *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 787–798, Apr. 2015.
- [3] H. Tu, H. Feng, S. Srdic, and S. Lukic, “Extreme fast charging of electric vehicles: A technology overview,” *IEEE Trans. Transport. Electrific.*, vol. 5, no. 4, pp. 861–878, Dec. 2019.
- [4] G. Kumar et al., “A privacy-preserving secure framework for electric vehicles in IoT using matching market and signcryption,” *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7707–7722, Jul. 2020.
- [5] Z. Garofalaki, D. Kosmanos, S. Moschoyannis, D. Kallergis, and C. Douligeris, “Electric vehicle charging: A survey on the security issues and challenges of the open charge point protocol (OCPP),” *IEEE Commun. Surveys Tuts.*, vol. 24, no. 3, pp. 1504–1533, Thirdquarter 2022.
- [6] T. Garg, N. Kagalwalla, P. Churi, A. Pawar, and S. Deshmukh, “A survey on security and privacy issues in IoV,” *Int. J. Electr. Comput. Eng.*, vol. 10, no. 5, 2020, Art. no. 5409.
- [7] A. Fiat and M. Naor, “Broadcast encryption,” in *Proc. Annu. Int. Cryptol. Conf.*, 1994, pp. 480–491.
- [8] C. Delerablée, “Identity-based broadcast encryption with constant size ciphertexts and private keys,” in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, 2007, pp. 200–215.
- [9] R. Sakai and J. Furukawa, “Identity-based broadcast encryption,” *Cryptol. ePrint Arch.*, 2007.
- [10] C. Gentry and B. Waters, “Adaptive security in broadcast encryption systems (with short ciphertexts),” in *Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn.*, 2009, pp. 171–188.
- [11] D. Boneh and M. Hamburg, “Generalized identity based and broadcast encryption schemes,” in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, 2008, pp. 455–470.
- [12] H. Xiong, Y. Zhao, L. Peng, H. Zhang, and K.-H. Yeh, “Partially policy-hidden attribute-based broadcast encryption with secure delegation in edge computing,” *Future Gener. Comput. Syst.*, vol. 97, pp. 453–461, 2019.
- [13] Y. Zheng, “Digital signcryption or how to achieve cost (signature & encryption) << cost (signature)+ cost (encryption),” in *Proc. Annu. Int. Cryptol. Conf.*, 1997, pp. 165–179.
- [14] M. Elhoseny and K. Shankar, “Reliable data transmission model for mobile ad hoc network using signcryption technique,” *IEEE Trans. Rel.*, vol. 69, no. 3, pp. 1077–1086, Sep. 2020.
- [15] N. Eltayieb, R. Elhabob, A. Hassan, and F. Li, “A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud,” *J. Syst. Archit.*, vol. 102, 2020, Art. no. 101653.
- [16] F. Li, X. Xin, and Y. Hu, “Identity-based broadcast signcryption,” *Comput. Standards Interfaces*, vol. 30, no. 1/2, pp. 89–94, 2008.
- [17] Y. Zhao, Y. Wang, Y. Liang, H. Yu, and Y. Ren, “Identity-based broadcast signcryption scheme for vehicular platoon communication,” *IEEE Trans. Ind. Informat.*, vol. 19, no. 6, pp. 7814–7824, Jun. 2023.
- [18] A. Elkhaili, R. Elhabob, and N. Eltayieb, “An efficient signcryption of heterogeneous systems for internet of vehicles,” *J. Syst. Archit.*, vol. 113, 2021, Art. no. 101885.
- [19] Q. Huang, D. S. Wong, and G. Yang, “Heterogeneous signcryption with key privacy,” *Comput. J.*, vol. 54, no. 4, pp. 525–536, 2011.
- [20] F. Li, H. Zhang, and T. Takagi, “Efficient signcryption for heterogeneous systems,” *IEEE Syst. J.*, vol. 7, no. 3, pp. 420–429, Sep. 2013.
- [21] S. Ma, Q. Huang, M. Zhang, and B. Yang, “Efficient public key encryption with equality test supporting flexible authorization,” *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 3, pp. 458–470, Mar. 2015.
- [22] S. Ma, “Identity-based encryption with outsourced equality test in cloud computing,” *Inf. Sci.*, vol. 328, pp. 389–402, 2016.
- [23] H. Xiong, H. Wang, W. Meng, and K.-H. Yeh, “Attribute-based data sharing scheme with flexible search functionality for cloud assisted autonomous transportation system,” *IEEE Trans. Ind. Informat.*, vol. 19, no. 11, pp. 10977–10986, Nov. 2023.
- [24] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*, 2004, pp. 506–522.
- [25] G. Yang, C. H. Tan, Q. Huang, and D. S. Wong, “Probabilistic public key encryption with equality test,” in *Proc. Cryptographers Track RSA Conf.*, Springer, 2010, pp. 119–131.
- [26] H. Xiong et al., “Heterogeneous signcryption with equality test for IIoT environment,” *IEEE Internet Things J.*, vol. 8, no. 21, pp. 16142–16152, Nov. 2021.
- [27] Q. Tang, “Towards public key encryption scheme supporting equality test with fine-grained authorization,” in *Proc. Australas. Conf. Inf. Secur. Privacy*, 2011, pp. 389–406.
- [28] Q. Tang, “Public key encryption supporting plaintext equality test and user-specified authorization,” *Secur. Commun. Netw.*, vol. 5, no. 12, pp. 1351–1362, 2012.
- [29] Q. Tang, “Public key encryption schemes supporting equality test with authorisation of different granularity,” *Int. J. Appl. Cryptogr.*, vol. 2, no. 4, pp. 304–321, 2012.
- [30] S. Ma, M. Zhang, Q. Huang, and B. Yang, “Public key encryption with delegated equality test in a multi-user setting,” *Comput. J.*, vol. 58, no. 4, pp. 986–1002, 2015.
- [31] K. Huang, R. Tso, Y.-C. Chen, S. M. M. Rahman, A. Almogren, and A. Alamri, “PKE-AET: Public key encryption with authorized equality test,” *Comput. J.*, vol. 58, no. 10, pp. 2686–2697, 2015.
- [32] H. Xiong, Y. Hou, X. Huang, Y. Zhao, and C.-M. Chen, “Heterogeneous signcryption scheme from IBC to PKI with equality test for WBANs,” *IEEE Syst. J.*, vol. 16, no. 2, pp. 2391–2400, Jun. 2022.
- [33] H. Xiong, Z. Qu, X. Huang, and K.-H. Yeh, “Revocable and unbounded attribute-based encryption scheme with adaptive security for integrating digital twins in Internet of Things,” *IEEE J. Sel. Areas Commun.*, vol. 41, no. 10, pp. 3306–3317, Oct. 2023.
- [34] L. Wang, Y. Lin, T. Yao, H. Xiong, and K. Liang, “FABRIC: Fast and secure unbounded cross-system encrypted data sharing in cloud computing,” *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 6, pp. 5130–5142, Nov./Dec. 2023.
- [35] I. Ali, T. Lawrence, A. A. Omala, and F. Li, “An efficient hybrid signcryption scheme with conditional privacy-preservation for heterogeneous vehicular communication in VANETs,” *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 11266–11280, Oct. 2020.
- [36] J. Malone-Lee, “Identity-based signcryption,” *Cryptol. ePrint Arch.*, 2002.
- [37] B. Libert and J.-J. Quisquater, “A new identity based signcryption scheme from pairings,” in *Proc. IEEE Inf. Theory Workshop*, 2003, pp. 155–158.
- [38] S. S. Siu-Ming, C. Yiu, L. C. Hui, and K. Chow, “Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity,” in *Proc. Int. Conf. Inf. Secur. cryptol.*, 2004, pp. 352–369.

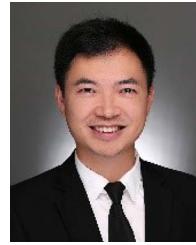
- [39] X. Boyen, "Multipurpose identity-based signcryption: A swiss army knife for identity-based cryptography," in *Proc. Annu. Int. Crypto. Conf.*, 2003, pp. 383–399.
- [40] L. Chen and J. Malone-Lee, "Improved identity-based signcryption," in *Proc. Int. Workshop Public Key Cryptography*, 2005, vol. 3386, pp. 362–379.
- [41] X. Pan, Y. Jin, Z. Wang, and F. Li, "A pairing-free heterogeneous signcryption scheme for unmanned aerial vehicles," *IEEE Internet Things J.*, vol. 9, no. 19, pp. 19426–19437, Oct. 2022.
- [42] Y. Cao et al., "Towards cyber security for low-carbon transportation: Overview, challenges and future directions," *Renewable Sustain. Energy Rev.*, vol. 183, 2023, Art. no. 113401.
- [43] H. Zhong, S. Zhang, J. Cui, L. Wei, and L. Liu, "Broadcast encryption scheme for V2I communication in VANETs," *IEEE Trans. Veh. Technol.*, vol. 71, no. 3, pp. 2749–2760, Mar. 2022.
- [44] C. Ge, Z. Liu, J. Xia, and L. Fang, "Revocable identity-based broadcast proxy re-encryption for data sharing in clouds," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 3, pp. 1214–1226, May/Jun. 2021.
- [45] Y. Cao, O. Kaiwartya, C. Han, K. Wang, H. Song, and N. Aslam, "Toward distributed battery switch based electro-mobility using publish/subscribe system," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 10204–10217, Nov. 2018.
- [46] A. Karati, S. H. Islam, G. P. Biswas, M. Z. A. Bhuiyan, P. Vijayakumar, and M. Karuppiyah, "Provably secure identity-based signcryption scheme for crowdsourced industrial Internet of Things environments," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2904–2914, Aug. 2018.
- [47] S. Niu, R. Dong, and L. Fang, "Certificateless broadcast signcryption scheme supporting equality test in smart grid," *PLoS One*, vol. 18, no. 9, 2023, Art. no. e0290666.



Yingzhe Hou received the B.S. degree from Northeast Forestry University, Harbin, China, in 2018, and the M.S. degree from the University of Electronic Science and Technology of China, Chengdu, China, in 2021. She is currently working toward the Ph.D. degree with the School of Cyber Science and Engineering, Wuhan University, Wuhan, China. Her research interests include public-key cryptography and privacy-preserving.



Yue Cao (Senior Member, IEEE) received the Ph.D. degree from the Institute for Communication Systems formerly known as the Centre for Communication Systems Research, University of Surrey, Guildford, U.K., in 2013. Further to the Ph.D. study, he had conducted a Research Fellow with the University of Surrey, and an Academic Faculty with Northumbria University, Newcastle upon Tyne, U.K., Lancaster University, Lancaster, U.K., and Beihang University, Beijing, China. He is currently a Professor with the School of Cyber Science and Engineering, Wuhan University, Wuhan, China. His multidisciplinary research focuses on the theme of ITS, including cyber security, wireless network, and service optimization. Prof. Cao has also been the Fellow of the British Computer Society, Royal Society of Arts, and Higher Education Academy.



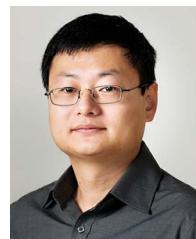
Hu Xiong (Senior Member, IEEE) received the Ph.D. degrees from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2009. He is currently a Full Professor with the UESTC. His research interests include public key cryptography and networks security.



Jiawen Kang (Senior Member, IEEE) received the Ph.D. degree from the Guangdong University of Technology, Guangzhou, China, in 2018. From 2018 to 2021, he was a Postdoc with Nanyang Technological University, Singapore. He is currently a Professor with Guangdong University of Technology. His research interests include blockchain, security, and privacy protection in wireless communications and networking.



Chuan Heng Foh (Senior Member, IEEE) received the M.Sc. degree from Monash University, Melbourne, VIC, Australia, in 1999, and the Ph.D. degree from the University of Melbourne, Melbourne, VIC, in 2002. He was a Lecturer with Monash University for six months. In 2002, he joined Nanyang Technological University, Singapore as an Assistant Professor till 2012. He is currently a Senior Lecturer with the University of Surrey, Guildford, U.K. He has authored or coauthored more than 100 refereed papers in international journals and conferences. His research interests include protocol design and performance analysis of various computer networks including wireless local area and mesh networks, mobile ad hoc and sensor networks, Internet of Things, 5G networks, and data center networks. He is an Associate Editor for IEEE ACCESS, IEEE WIRELESS COMMUNICATIONS, and *International Journal of Communications Systems*. He is also the Vice-Chair (Europe/Africa) of IEEE Technical Committee on Green Communications and Computing.



Changyu Dong (Member, IEEE) received the Ph.D. degree from Imperial College London, London, U.K. He is currently a Professor with the Institute of AI and Blockchain, Guangzhou University, Guangzhou, China. He has authored more than 50 publications in international journals and conferences. His recent work focuses mostly on designing practical secure computation protocols. The application domains include secure cloud computing and privacy preserving data mining. His research interests include applied cryptography, data privacy, AI security, and blockchain.