A Lightweight Privacy-preserving Path Selection Scheme in VANETs

Guojun Wang[1,2], Huijie Yang[3,4]*

[1] *Yancheng Polytechnic College, China*
[2] *School of Electronics & Information Engineering, Nanjing University of Information Science and Technology, China*
[3] *School of Computer Science, Nanjing University of Information Science and Technology, China*
[4] *School of Computing and Information Systems, Singapore Management University, Singapore*
113097096@qq.com, hjyang03@126.com

Abstract

With the rapid development of edge computing, artificial intelligence and other technologies, intelligent transportation services in the vehicular ad hoc networks (VANETs) such as in-vehicle navigation and distress alert are increasingly being widely used in life. Currently, road navigation is an essential service in the vehicle network. However, when a user employs the road navigation service, his private data maybe exposed to roadside nodes. Meanwhile, when the trusted authorization sends the navigation route data to the user, the user can obtain all the road data. Especially, other unrequested data might be related to the military. Therefore, how to achieve secure and efficient road navigation while protecting privacy is a crucial issue. In this paper, we propose a privacy-preserving path selection protocol that supports a token as the object in the oblivious transfers, which effectively reduces the communication overhead. In addition, a lightweight dual authentication and group key negotiation protocol is provided to support dynamic joining or leaving of group members. Moreover, it can guarantee the security of forward data. After experimental analysis, the proposed protocol has high security and efficiency.

Keywords: Privacy protection, Oblivious transfers, Group key agreement, VANETs

1 Introduction

With the rapid development of vehicular ad hoc networks (VANETs), intelligent transportation services, such like traffic management and road navigation are become more and more reliable [1-3]. For the purpose of establishing real-time dynamic information services, smart transportation primarily makes use of new generation information technology, such as cloud computing, edge computing, and artificial intelligence [4-5]. In particular, navigation is an indispensable essential service in smart transportation. The vehicle network is typically composed of three basic components: the vehicle, the road side unit (RSU), and the trusted authority (TA) [6]. Strong computation and storage capabilities enable TA to transmit or gather a variety of data kinds to the car through RSU. He has a big region for receiving signals. RSU is a unit node mounted to the side of the road that helps cars transmit data to TA. RSU's signal coverage region is less extensive than TA's [7]. When traveling, cars will seek congested road segments from RSU or TA in an effort to avoid them as soon as possible. The VANETs will gather real-time data on the state of the roads and provide the user with the pertinent information. However, there is a chance that private information like the location of the vehicle, the number of miles driven, and driving habits will be exposed when smart cars like Tesla and XPENG use VANETs [8]. Therefore, privacy protection issues need to be considered when providing smart transportation services such as road navigation.

Imagine a situation when a vehicle requests a navigation path from a TA in VANETs. The request contains information on the vehicle's ID, its location, its destination and road preferences, as well as other sensitive data. In general, a vehicle receives the computed n navigation paths from the TA and is free to select the preferred route. However, under the situation as it is now written, it is possible for malicious users to have access to both vehicle and TA privacy. On the one hand, the TA can still access the user's private data after decrypting the ciphertext, even if the vehicle encrypts the data before sending it to the TA. On the other hand, the user receives the sent navigation routes and can discover alternative highways. It is worth noting that other road data may also contain information on the privacy of other vehicles, etc. Furthermore, storing n routes required waste storage space. Therefore, three issues should be considered.

1.1 Motivations of This Paper

Firstly, in general, a driver does not inform all routes to his destination based on the existing experience. Meantime, he also desires to keep abreast of road congestion. In this case, the driver sends a navigation request to TA, which contains the origin and destination of vehicle and road characteristics. However, on the one hand, the driver's habits, privacy, and vehicle trajectory can be captured by TA. TA has an ability to conjecture habits of driver's navigation according to the revealed privacy. Critically, private information can be collected and sold to some organizations. On the other hand, navigation routes have data from smart transportation

*Corresponding Author: Huijie Yang; E-mail: hjyang03@126.com
DOI: 10.53106/160792642023072404004

services and sensitive information such as bridges, subways, roads, and ports. If the privacy of navigation routes is not protected, drivers can obtain all the information about routes.

Secondly, group members generate session keys with the TA. If a member quits or joins the group, the revoking user should not be able to access the data forward or after. Otherwise, the data will be exposed to the revoking user. Also, the newly joined user cannot know any previous data. Therefore, the proposed protocol needs to support group members to join or leave dynamically, and to guarantee the confidentiality of the data.

Thirdly, during road navigation, all routes are usually sent to drivers. This approach not only exposes the privacy in the routes. Also, n navigation routes are returned to a driver, which generates a large amount of computational overhead and communication overhead.

1.2 Our Contributions

In this paper, a lightweight navigation path selection scheme in VANETs is presented based on the novel dual authentication algorithm and oblivious transfers algorithm, which sends an optimal and needed path to user and protects the privacy of all entities. In addition, the scheme can provide users with dynamic join or leave features and dual authentication service.

1) ***A path selection scheme supporting privacy-preserving is proposed.*** To avoid exposure the privacy of communication entities, this scheme is designed based on 1-out-of-n oblivious transfers (OT_n^1) between vehicle (denoted as user-side) and TA (denoted as server-side). Specifically, during the process of a user interacting with a TA for n navigation paths, a user requests one navigation path from n paths to TA, then he only obtains a requested path and has no information about $n-1$ paths, while TA cannot know any information about the request data.

2) ***Dual authentication and group members dynamically joining or leaving can be provided in this scheme.*** The novel and lightweight dual authentication algorithm can be performed among users, RSUs and TAs, which guarantees only the authenticated entities to participate in the follow-up algorithms. Moreover, the presented group key agreement algorithm supports the members joining or leaving dynamically and forward secrecy. That is, the malicious user cannot fake the valid identity and attempt to join in the group and reveal the message from TA.

3) ***The computation and communication of our scheme are effectively reduced.*** The encrypted route message is not the object of oblivious transfer, since transmitting encrypted route message between user and TA will cause a large communication overhead. In the proposed OT_n^1, the token is the object to transmit. The performance analysis and evaluation are illustration for dual authentication algorithm and 1-out-of-n oblivious transfers algorithm with other protocols. It has proved that the performance and efficiency of this paper have been improved.

1.3 Organization

The reset of this paper is organized as follows. The related work about some privacy-preserving path selection schemes is introduced in Section 2. Some concepts about oblivious transfers and smooth projective hash function are described in Section 3. The system model and adversary model are presented in Section 4. A lightweight and privacy-preserving path selection scheme is proposed in Section 5. The security and performance analysis are illustrated in Section 6 and Section 7, respectively. Section 8 concludes the proposed scheme.

2 Related Work

Intelligent transportation services are rapidly becoming more common due to the ongoing promotion of electric vehicles [9-11]. The service of road navigation is crucial in intelligent transportation. Bhatnagar *et al.* [12] applied the cumulative distribution function and probability density function to design a best path selection scheme. Ubarhande *et al.* [13] proposed a secure path selection scheme based on distributed delegation, which permitted the authenticated node to join in the active path. Based on the scheme [12], Xu *et al.* [14] proposed a novel max weighted-harmonic-mean schemes to assist with path navigation. However, the privacy of the receiver and sender is not protected in existing solutions.

In VANETs, the oblivious transfers technology is employed to protect the privacy of interaction entities [15-16]. To protect the users' privacy during VANET's feature matching, an efficient k-out-of-n oblivious transfers was proposed by Wang *et al*. [17], and it was adopted to give a PSI protocol with equality test. To address the privacy of location data of user, a privacy-preserving location-based scheme is proposed by Yadav *et al.* [18] to protect some privacy, such as the query privacy of the user, information content of the location server, and location information, etc. Liang *et al.* [19] desired to protect the privacy of RSUs and vehicles, and they proposed a route planning scheme in VANETs with assisting of certification authority. Moreover, the dual authentication and group key agreement technologies are also the essential functions in VANETs. Vijayakumar *et al.* [20] proposed a dual authentication algorithm among the vehicles, RUS and TA to verify the identities of entities for following steps. Then, TA according to the user authentication list generated the group session key for vehicles, while it distinguished primary user and secondary user for protect the security of message. However, the scheme [20] cannot resist the replay attack and masquerade attack, which was figured out by Tan *et al.* [21]. They pointed out the previously request messages which could be reused by malicious users. To address this problem, they proposed a novel dual authentication scheme. Avoiding the real-time data to be collected by devices, Vinoth *et al.* [22] employed the Chinese remainder theorem and secret sharing technology to design a secure multifactor authenticated key agreement scheme, which could withstand many known attacks. However, the above schemes did not consider about the flexibility of authentication key agreement. Tan *et al.* [23] proposed a flexible authentication mechanism with the dynamic access policy based on secret sharing technology, which provided anonymity for users. However, some schemes have difficulty

balancing security and efficiency, specifically, the excessive overhead generated by privacy protection affects the efficiency of protocols in VANETs.

3 Preliminaries

In this section, some algorithms or definitions are presented, that is 1-out-of-n oblivious transfers protocol, smooth projective hashing function and Chinese remainder theory. These technologies are applied in the proposed scheme.

3.1 1-out-of-n Oblivious Transfers

1-out-of-n oblivious transfers protocol involves two entities: receiver and sender. The sender inputs n messages and receiver inputs one request r. After executing OT_n^1 protocol, the receiver obtains one message from n. It is clear from the security regulations of the OT protocol that the privacy of communication entities, receiver and sender, is commanded to protect. That is, a sender returns n messages to receiver, yet he does not know anything about the request. Meanwhile, a receiver only can obtain one message without learning any information about $n - 1$ messages. We describe a OT_n^1 protocol designed by Naor *et al.* [24] as follows.

Input: Sender inputs $\{M_1, M_2, \ldots, M_n\}$, where $M_i \in \{0,1\}^m$, $n = 2^l$ and $i \in [n]$. Receiver inputs the request $r \in [n]$.

Output: Then, receiver desires to learn M_r.

Step 1: Sender randomly selects l pairs of keys $K = \{(K_1^0, K_1^1), (K_2^0, K_2^1), \ldots, (K_l^0, K_l^1)\}$, where K_j^{bj} is a a-bit string key and $j \in [l]$ hold. Sender computes $CT_i = M_i \oplus (\oplus_{j=1}^{l} F_{K_j} b_j(i))$, where $F(\cdot)$ is a pseudo-random function. Then, sender returns CT_i to receiver.

Step 2: Sender and receiver perform a 1-out-of-2 oblivious transfers protocol based on K. Receiver would like to obtain K_j^{bj}, when he requires to get M_r.

Step 3: Receiver computes $M_r = CT_i \oplus (\oplus_{j=1}^{l} F_{K_j} b_j(i))$ and obtains the request message M_r.

3.2 Smooth Projective Hashing Function

The concept of smooth projective hashing function is first proposed by Cramer *et al.* [25], which has a pair of keys. This function computes the hash value in two manners. Firstly, it calculates the hash value h_h by using a hash key. Secondly, it calculates the projective hashing value h_{ph} of some subset by employing a projective key. Finally, $h_h = h_{ph}$ holds. The specifics steps are as follows.

Setup(1^k): Input a security parameter k. Setup algorithm generates the system parameter *param*.

GenHashKey(*param*): GenHashKey algorithm randomly generates a hash key h_k.

GenProKey(h_k, *param*, w): GenProKey algorithm generates a projective key *hp* by employing key h_k.

HashVa(h_k, *param*, w): HashVa algorithm generates a hash value h_h by using key h_k.

ProHash(h_p, *param*, w): ProHash algorithm generates a projective hashing value h_{ph} by applying key h_p.

For all hashing keys and projective keys, the formular HashVa(h_k, *param*) = *ProHash*(*hp*, *param*) established based on witness $w \in L$, where L belongs to the NP.

3.3 Chinese Remainder Theorem

Suppose $n_1, n_2, \ldots, n_k$ are positive integers, and they are mutually prime. If $M = \prod_{i=1}^{k} n_i$ establishes, then a system of congruent equations (1) exists.

$$\begin{cases} a_1 \bmod n_1 \equiv x \\ a_2 \bmod n_2 \equiv x \\ \quad \cdots \\ a_k \bmod n_k \equiv x \end{cases}. \tag{1}$$

The mode M has a unique value, $x \equiv (\frac{M}{n_1} e_1 a_1 + \frac{M}{n_2} e_2 a_2 + \ldots + \frac{M}{n_k} e_k a_k) \bmod M$, where e_i is satisfied with $\frac{M}{n_i} e_i \equiv 1 \bmod n_i (i \in [k])$.

4 System Model and Adversary Model

4.1 System Model

In VANETs, three entities are composed of system model, users/vehicles, road site unit (RSU) and trusted authority (TA). The system model of a lightweight privacy-preserving path selection scheme is presented in Figure 1.

Vehicles, RSUs and TAs form a vehicle network. At initial phase, vehicles and RSUs need to register their respective identities with the TA. To prevent identity leakage of entities, dummy identities are assigned to vehicles, RSUs and TAs during the initialization phase to protect privacy when they communicate. Subsequently, vehicle-RSU and RSU-TA authenticate each other, generating a registered list at the TA. With this list, the TA generates a group session key. Obviously, only the users in this list can obtain this session key. When a user withdraws or joins, the TA regenerates the group session key to ensure that the data is not leaked. The most important function is the navigation path access. When a user sends a navigation request to the RSU, the RSU will return n paths that meet the conditions to the user. But the user can only get one of them and cannot get any information about the other $n - 1$ paths.

Trusted Authority (TA): TA is mainly responsible for the registration, dual authentication and group key agreement phases between the vehicle, RSU and TA. TA is a fully trusted entity. It uses the information in the registration phase to complete the dual authentication with vehicles and RSUs, which can effectively avoid malicious vehicles from joining the VANETs. When a vehicle changes from State A to State B, it needs to re-register with the TA. And the group session key corresponding to State B cannot be obtained immediately. In addition, the TA generates the group session key based on the user registration form. It can identify malicious users quickly.

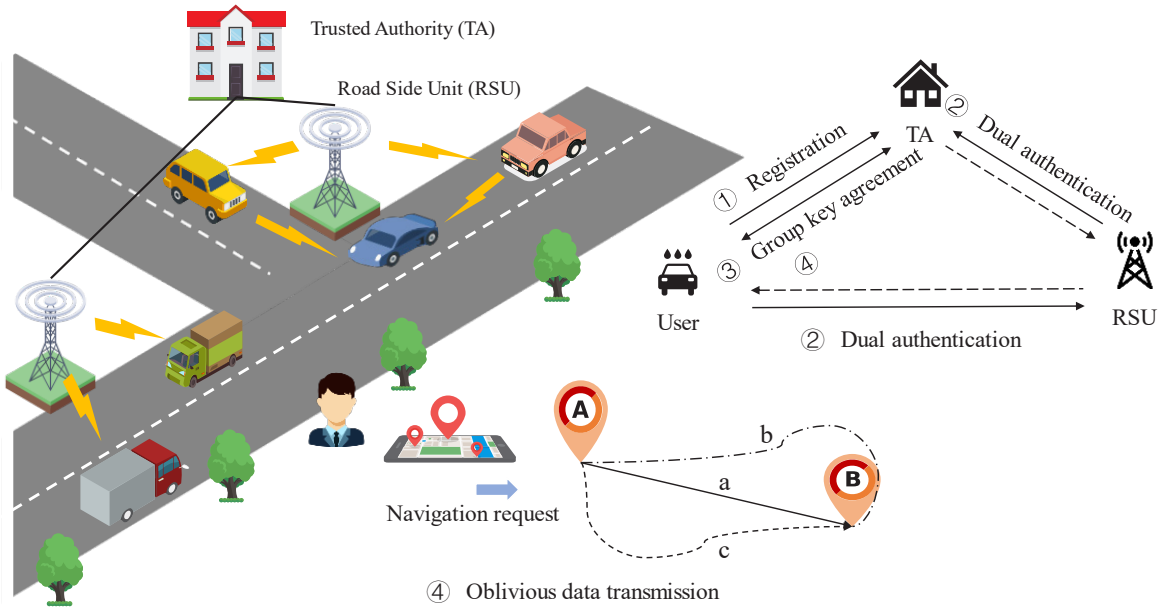

Figure 1. System model

Road Site Unit (RSU): The RSU is managed by the TA and is the intermediate entity of the VANETs. That is, the RSU is the bridge that connects vehicles and TAs. In the dual authentication phase, the RSU assists the TA and the vehicle to complete the identity authentication between each other. In the navigation route transmission phase, the encrypted routes are stored in the TA, and keys corresponding to routes are stored in RSU. Then, RSU and vehicles execute the proposed OT protocol, n keys are transmitted obliviously to a vehicle so that this vehicle can decrypt its request route after obtaining one key.

Vehicle: Every vehicle is embedded with a RSU in the VANETs. And it also can communicate with other vehicles and RSUs.

4.2 Algorithm Definition

Registration Phase: $U_{key} \leftarrow R_e(para, id_{TA})$. When, a vehicle travel in the range of TA, then TA generates its dummy identity id_{TA} to a user. User inputs the dummy identity of TA to compute auxiliary messages ($preK$, $preM$) which assists to transmit user's key U_{key}. The key of user U_{key} is mainly applied in the dual authentication to verify user's identity, which prevents a malicious user to forge the real identity of honest user.

Dual Authentication Phase: $dul - Auth_U \leftarrow D_u(\{timestamp\}, Auth_u, Auth_R, Auth_{TA}, dul - Auth_R)$. The user, RSU and TA accomplish the dual authentication with each other in this phase. A user computes parameter $preAuth_u$ and $Auth_u$ in which includes his personal information for verifying at TA. He sends the ciphertext $Auth_u$ to RSU. RSU re-encrypts $Auth_u$ with its dummy identity and sends $Auth_R$ to TA. TA employs user's and RSU's keys where are from the registration phase to decrypt ciphertext $Auth_u$ and checks $preAuth_u^{'} \overset{?}{\Leftrightarrow} preaAuth_{TA}^{'}$. The one-way authentication $vehicel \rightarrow RSU \rightarrow TA$ has completed. Then, the smooth projective hash function is applied in TA to compute $preAuth_{TA}$. Employing the dummy identity of TA encrypts $preAuth_{TA}$ to generate $Auth_{TA}$ and sends to RSU. RSU re-encrypts the ciphertext to compute $dul - Auth_R$ for user. Finally, the user utilizes the feature of the SPH function to verify TA's identity to finish the dual authentication.

Group Key Agreement Phase: $KA_{key} \leftarrow GKA(para', L)$. TA determines the users contained in the list L, i.e., the group users. Using the Chinese remainder theorem, TA distributes the computed group session key to the group users. When a user joins or withdraws, the list L is updated. TA generates a new session key based on list L' to prevent a malicious user from being able to access the previous data.

Oblivious Data Transmission Phase: $M_e \leftarrow ODT(\{M\}_n, KA_{key}, token_j)$. The navigation function is provided via embedding the oblivious transfers technology in our scheme. A user sends a message to TA with the information containing the location of origin and destination. TA calculates and encrypts paths via using a $token_j$, broadcasts n paths for vehicles. However, not all vehicles can obtain one or n paths. The vehicle should receive a $token_j$ corresponding a path by performing $ODT(\cdot)$. Finally, a user employs this token to decrypt the ciphertext to obtain the required path.

4.3 Adversary Model

The adversary model determines the capabilities of the attacker, which is defined as follows.

1) The adversary A_1 might purposefully repeat to send the valid messages for many times, which can disturb the transmission between users, RSUs and TAs. This kind of adversary is mainly found in the dual authentication phase, trying to spoof the RSU or TA.

2) The adversary A_2 wants to obtain any information about the request r so that he can infers a monitored user's

habit. He simulates and selects a request r' to run the proposed oblivious transfers algorithm, which tries to figure out the relationship between r' and $token'$.

3) The adversary A_3 attempts to reveal the privacy about $n-1$ paths. He selects sCT_j to perform oblivious transfer and tries to figure out the relationship between sCT_j and $token'$.

5 The Proposed Scheme

To support a lightweight and privacy-preserving path selection scheme in VANETs, we mainly design a novel dual authentication algorithm and a lightweight 1-out-of-n oblivious transfers algorithm. The proposed scheme is divided into four phases, in which the registration phase is described in Section 5.1, the dual authentication phase is presented in Section 5.2, the group key agreement phase is stated in Section 5.3 and the oblivious data transmission is illustrated in Section 5.4.

5.1 Registration Phase

Generate the dummy identity of user (vehicle), RSU and TA, applied in the following phases to protect their real identity [26-27]. Select randomly a number $a \in Z_q^*$. Compute and broadcast the dummy identity of TA $id_{TA} = g^a$ via a secure channel, where g is the generator of Z_q^*. Similarly, the dummy identity of user (id_u) and RSU (id_{RSU}) are generated by TA. Obviously, the correspondence between the dummy identity and the real identity only is known by TA, and for a malicious user, he still has no way to learn any information of the real identity of user or RSU.

1) Firstly, a user arrives in the range of TA and inputs some personal information, i.e., name n_a, identity id_u, mileage v_{km}, etc. Those information as the fingerprint of user are encrypted and sent to TA. A user randomly chooses a key $key \in \{0, 1\}^l$, where $l = 256$ bits. Then, he encrypts the communication key with the dummy identity id_{TA}, denoted as $preK = id_{TA} \oplus h(id_{TA} \| key)$, where supposes a trapdoor hash function that is implemented by a secure symmetric encryption scheme $h: \{0, 1\}^* \rightarrow \{0, 1\}^l$. After that, he encrypts his personal information with key, the ciphertext is presented as Eq. (2).

$$preEM = E_{key}(n_a \| id_u \| v_{km} \| v_{ty}). \tag{2}$$

The user sends ciphertexts ($preK$, $preM$) to TA.

2) Secondly, to obtain key, TA computes $preK' = preK \oplus id_{TA}$, uses a trapdoor hash function and identity id_{TA} to decrypt ciphertext $h(id_{TA} \| key)$. Then, TA decrypts $preEM$ and records the user's personal information into the List L, the Eq. (3) denotes the decrypted data.

$$preDM = D_{key}(E_{key}(n_a \| id_u \| v_{km} \| v_{ty})). \tag{3}$$

Then, TA select a new key $U_{key} \in \{0, 1\}^l$ and employs the trapdoor hash function to encrypt U_{key}. TA sends the ciphertext $preKA$ to a user, described as $preKA = id_{TA} \oplus h(id_{TA} \| U_{key})$.

3) Finally, a user decrypts $preKA$ and reveals U_{key}. Each user and TA maintain key U_{key} for performing the dual authentication and group key agreement phases.

5.2 Dual Authentication Phase

When a user desires to create a communication channel with RSU, he is commanded to compute $preKA'$ and send to TA. TA makes sure $preKA'$ is equal to $preKA$, which $preKA$ has stored in TA in the registration phase. If two values match, then a user can communicate with RSU. Otherwise, this user is judged to be a malicious user and expelled to the VANETs. Figure 2 shows the process of the dual authentication phase.

1) The user randomly selects a number $b \in Z_q$, and set a time stamp t_1. He applies a trapdoor hash function as the secure symmetric algorithm to encrypt b, denoted as $preAuth_u = h(U_{key} \| b)$. Then, he uses his personal information to encrypt $preAuth_u$ and transmits ($Auth_u$, t_1) to RSU. Eq. (4) presents the ciphertext $Auth_u$.

$$Auth_u = E_{key}(preAuth_u \| id_u \| b) \oplus t_1 \oplus id_{TA}. \tag{4}$$

2) RSU sets a time stamp t_2 and encrypts $Auth_u$ with its dummy identity, denoted as Eq. (5). Then, RSU forwards ($Auth_R$, t_2) to TA.

$$Auth_R = E_{key_{RSU}}(E_{key}(preAuth_u \| id_u \| b) \oplus t_2 \oplus id_{TA}) \oplus id_{RSU}. \tag{5}$$

3) Supposing $f(\cdot)$ is a smooth projective function and $\beta(\cdot)$ is a projective key function. TA decrypts the ciphertext $Auth_R$ with a RSU's key key_{RSU} which has stored both in RSU and TA in registration. The transmission of key_{RSU} likes U_{key}. Eq. (6) and Eq. (7) are denoted the decryption via using RSU's key key_{RSU} and user's key key, respectively.

$$DeAuth_R = D_{key_{RSU}}(Auth_R). \tag{6}$$

$$DeAuth_u = D_{key}(E_{key}(preAuth_u \| id_u \| b)). \tag{7}$$

TA employs the decrypted message $preAuth_u$ to computes $preAuth'_{TA} = h(preAuth_u)$, and it also uses the stored key U_{key} to calculate $preAuth_u' = h(hU_{key} \| b))$. TA verify the equation $preAuth_u' \stackrel{?}{\Leftrightarrow} preaAuth_{TA}'$ is valid. If the above equation holds, then the one-way authentication (from a user to TA) is implemented and it attempts to begin another one-way authentication (from TA to a user). Otherwise, the dual authentication algorithm aborts.

Furthermore, TA sets a time stamp t_3. Applying the smooth projective hash function computes $preAuth_{TA} = f(preAuth_u; \beta(U_{key}); id_u)$. Then, it encrypts $preAuth_{TA}$ with its dummy identity, described as Eq. (8). TA sends ($Auth_{TA}$, t_3) to RSU.

$$Auth_{TA} = E_{key}(preAuth_{TA} \,||\, id_{TA}) \oplus t_3. \tag{8}$$

4) RSU utilizes his dummy identity and a new time stamp t_4 to encrypt $Auth_{TA}$, which demonstrates as Eq. (9). Transmit ($dul - Auth_R$, t_4) to user.

$$dul - Auth_R = E_{key_{RSU}}(E_{key}(preAuth_{TA} \,||\, id_{TA}) \oplus t_4) \oplus id_{RSU}. \tag{9}$$

5) The user applies the smooth projective hash function to compute $dul - Auth_U = H_{U_{key}}(preAuth_u)$ for checking Eq. (12). In addition, he decrypts $dul - Auth_R$ via key_{RSU} and key for twice, presented as Eq. (10) and Eq. (11). If Eq. (12) establishes, the dual authentication algorithm is accomplished. What's more, the user, RSU and TA can transmit with each other. Otherwise, the proposed scheme aborts.

$$dul - DeAuth_R = D_{key_{RSU}}(E_{key_{RSU}}(E_{key}(preAuth_{TA} \,||\, id_{TA}) \oplus t_4)). \tag{10}$$

$$dul - DeAuth_U = D_{key}(E_{key}(preAuth_{TA} \,||\, id_{TA})). \tag{11}$$

$$dul - Auth_U \overset{?}{\Leftrightarrow} preaAuth_{TA}. \tag{12}$$

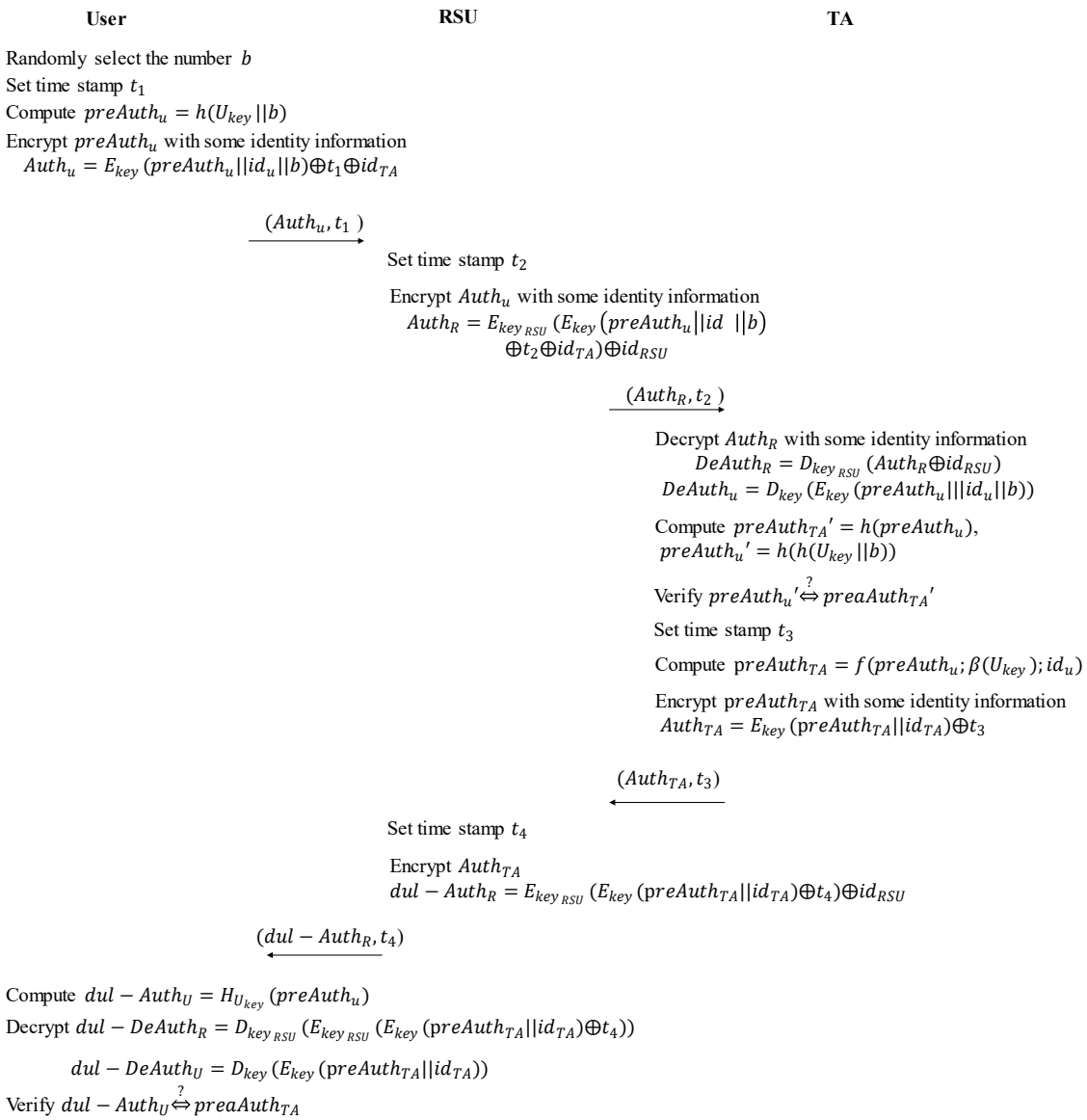

Figure 2. The process of dual authentication phase

5.3 Group Key Agreement Phase

Group session key can only be distributed to users who have stored data in List L at TA, as we stated in the system model. In addition, the group session key is employed in the oblivious data transmission to assist a user with obtaining the request path. TA generates the session key to obey the following steps.

1) TA computes $\alpha = \prod_{i=1}^{m}(U_{key_i})$. Each user's key U_{key} has transmitted during registration phase, $i \in [m]$ holds and m presents the number in the group. It calculates $\gamma_i = \frac{\alpha}{U_{key_i}}$ and $\gamma_i \cdot \delta_i \equiv 1 mod\ U_{key_i}$. After that, TA computes $\eta = \sum_{i=1}^{m}(\gamma_i \cdot \delta_i)$. It randomly chooses a number KA_{key} as a new session key for m users. Subsequently, TA computes and broadcasts the message $\theta = KA_{key} \cdot \eta$ to m users.

2) Each user extracts a session key by computing this equation $KA_{key} = \theta\ mod\ U_{key_i}$.

3) A user can join or leave a group using the group key agreement algorithm that was created. Therefore, two cases can be happened in VANETs.

- List L deletes a user U_{rev} from it, when user U_{rev} leaves or withdraws from this group. TA computes a new η', denotes as $\eta' = \eta - \gamma_{rev} \cdot \delta_{rev}$. Note that TA selects a new conference key KA'_{key} for a new group. Then, TA computes and broadcasts a new θ', describes as $\theta' = KA'_{key} \cdot \eta'$. Subsequently, each user in the new group computes $KA'_{key} = \theta'\ mod\ U_{key_i}$ to reveal a session key.
- List L adds a new user U_{add} who has implemented the dual authentication. TA computes a new η', $\eta' = \eta + \gamma_{add} \cdot \delta_{add}$. Note that TA randomly chooses a new conference key KA''_{key} for a new group. After that, TA computes and transmits θ'' to each user in the new group, where $\theta'' = KA''_{key} \cdot \eta''$ holds. The user reveals the group session key from θ''.

4) Whether a user join or leave this group, the forwards ciphertexts should be encrypted again via using a new group session key to ensure the confidentiality of data. Therefore, the re-encrypted ciphertext $CT_{re} = E_{KA''_{key}}(M)\cdot$ should be computed by TAs. In addition, in the oblivious data transmission phase, $token_j$ is applied to encrypt the messages. Once a user joins or leaves the group, the previously tokens are deleted. And, based on the define of oblivious transfer, a user only can obtain his requested message without others.

5.4 Oblivious Data Transmission Phase

Consider this scenario: a user wants to drive at Place A, so he sends TA a require. Meantime, TA maybe expose all the paths to each user, since paths are encrypted by using a session key. Thus, both the request user and others can reveal all paths, they all have this session key after performing group key agreement algorithm. Furthermore, the requested user's privacy, such as location and Place A, will be leaked to other users. Therefore, we encrypt the navigation paths with the aid of some tokens. The process of oblivious data transmission phase is presented in Figure 3, which implements to send the requested navigation path to a user. Those tokens contain some necessary information, i.e., location data, destination place, navigation preferences and so on. They are transmitted from TA to RSU by a secure channel. TA employs $token_j$ to encrypt n messages M_j, denotes as $CT_j = E_{token_j}(M_j), j \in [n]$.

1) Select three number randomly x, y, $c \in Z_q^*$ and g is a generator of Z_q^*. The user chooses an input $e \in [n]$ and generates the request $r = x^e \cdot y^c$. He transmits r to RSU.

2) RSU computes and sends $sCT_j = token_j \oplus h((\frac{r}{x^j})^{KA_{key}})$ to a user, where $j \in [n]$ holds.

3) The user computes $sCT_e = sCT_j \oplus h(y^{c \cdot KA_{key}})$. He obtains one path from n paths without learning any information about $n-1$ path. Finally, he employs his token to decrypt the ciphertext sent from TA, denotes as $M_e = D_{token_j}(CTe)$. In addition, TA is unable to determine which user paths are necessary.

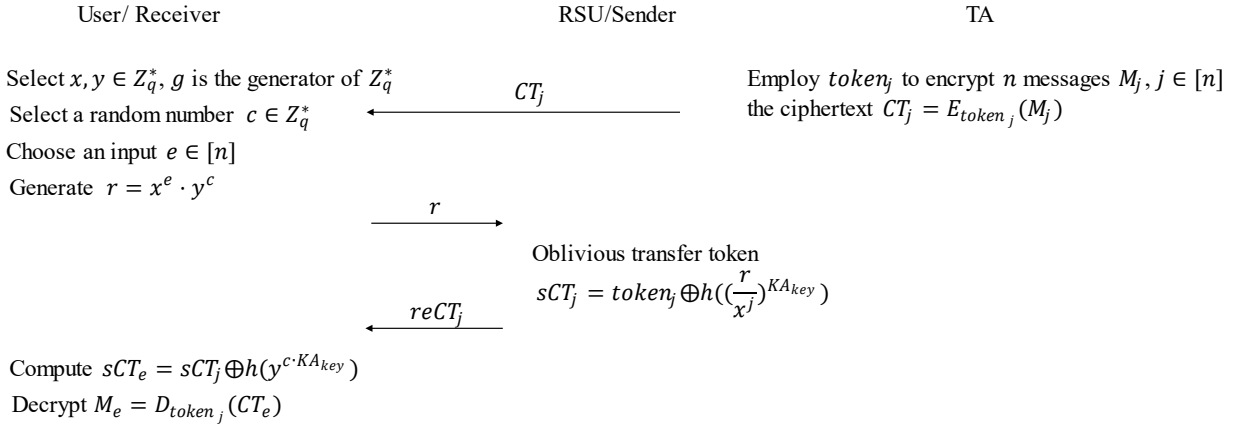

Figure 3. The process of oblivious data transmission phase

6 Security Analysis

In this section, we analyze the strength of the proposed navigation path selection scheme under the adversary model stated in Section 4.3.

6.1 Resistance to Replay Attack

As we have presented in Section 4.3, an adversary A_1 can intercept the sent messages to revise they, then resends the revised message to RSU or TA. However, time stamps are applied in our dual authentication, which can protect the messages from the replay attack and ensure the effectiveness of message. For example, in case of the dual authentication, an adversary A_1 observes and modifies the ciphertext $Auth_R$ to $Auth'_R$, since he forges a dummy identity id'_{RSU} and attempts to pretend a real RSU. However, the time stamp is used in the proposed algorithm to keep a cache of recently messages. TA compares a received message with a recent message through this time stamp, which $Auth_R = Auth'_R$ holds or not. Obviously, TA can discern the revised message and has an ability to resist the replay attack.

6.2 Receiver Security

The paths have been encrypted via using $token_j$, and ciphertexts are broadcasted by TA. Meantime, user as a receiver and RSU as a sender perform oblivious transfers algorithm, which helps a receiver to obtain one path from n path. However, an adversary A_2 acts as a sender to interact with a challenger. The adversary A_2 selects a random number $e' \in [n]$ and generates the request r'. Then, sCT_j can be queried by A_2 adaptively for $n - 1$ times at most. The adversary A_2 selects two requests r_0, r_1. The challenger randomly chooses $b \in \{0, 1\}$ and generates sCT_0, sCT_1. And the adversary outputs his guesses b'. Suppose that there is a probabilistic polynomial time who can break the receiver security with a non-negligible advantage ϵ. In addition, the probability of an adversary A_2 successfully guessing correctly is 1/2. Because only one request belongs to n, the other one is a forged request. If $b = b'$, the adversary wins. However, the probability of he successfully guessing b' from n is $Adv_{A_2} = \left(\frac{1}{2n}\right)^{\epsilon}$.

6.3 Sender Security

The oblivious transfers protocol commands that a receiver only can obtain one path which has been asked by himself. Meanwhile, a receiver cannot reveal other paths from the transmission messages. If the protocol obeys the above requirement, it is said that the sender's privacy has been protected. The adversary A_3 plays a role of a receiver and the challenger acts as a sender. The adversary A_3 send the request r to the challenger, and he can query about the $token_j$ adaptively for at most $n - 2$ times. The adversary sends sCT_j to challenger, then the challenger sends $token_j$ back. After that, the adversary outputs two same strings sCT_0 and sCT_1 to the challenger. The challenger computes sCT_b and sends back to adversary A_3. The adversary A_3 outputs b', if $b = b'$, A_3 wins. However, if the adversary wins this game, then IND-CPA security cannot be guaranteed. Therefore, the probability of adversary wining is $Adv_{A_3} = \left|Pr - \frac{1}{2}\right| \ll \epsilon$.

7 Performance Analysis and Evaluation

7.1 Performance Analysis

Four phases are contained in our proposed scheme, registration phase, dual authentication phase, group key agreement phase and oblivious data transmission phase. Note that, in order to protect the privacy of users and RSUs, our scheme design a novel 1-out-of-n oblivious transfer algorithm to transmit tokens, which inevitably introduces some communication overhead. However, the proposed protocol has effectively reduced the communication overhead compared to exposing the privacy or transmitting the ciphertext directly. Table 1 shows the comparison of each phase.

Table 1. The comparison of four phases

Phases	Overhead	*
Registration	$T_p + 2T_h + 2T_{ED}$	-
Dual authentication	$5T_h + 8T_{ED}$	-
Group key agreement	$T_m + T_{mod}$	*B*
Oblivious transfers	$2T_p + 2nT_h + (n+1)T_{ED}$	*B*

Let T_p denote a power operation time, T_h present a hash function time, T_{ED} state an encryption or decryption operation time, T_m introduce a multiplication operation time, T_{mod} describe a mod operation time, * denote communication complexity and *B* present broadcast.

In the registration phase, the computation overhead is $T_p + 2T_h + 2T_{ED}$. The overhead of XOR operation is very small, which is ignored in this paper. To ensure the confidentially of data, the encryption and decryption algorithms are employed in the dual-authentication phase. And the overhead of this phase is $5T_h + 8T_{ED}$. The Chinese Remainder theorem is applied to update the group session key which costs $T_m + T_{mod}$. In the oblivious transfer phase, n messages are sent to a user and these messages are needed to decrypt by a user to obtain the requested data, which costs $2T_p + 2nT_h + (n+1)T_{ED}$.

7.2 Performance Evaluation

The proposed 1-out-of-n oblivious transfers algorithm is the mainly contribution. We have evaluated this algorithm by using the python language under a desktop computer. The performance of this desktop computer is described as follows.

- CPU: Intel (R) Core (TM) i7-10700 CPU @2.90GHZ
- RAM: 16.0GB
- System: Windows 10, 64-bit

In general, the transmission message is the encrypted data. In this scheme, it should be the navigation paths. We set the length of ciphertext be 2048-bit. However, to consider about the overhead and storage, we employ the token to encrypt navigation paths and oblivious transfer the token

which only has 256-bit. Figure 4 shows the comparison of the computation overhead under 2048-bit and 256-bit data. Figure 4(a) describes the hash operation time in 1-out-of-n oblivious transfers algorithm. Figure 4(b) presents the symmetric encryption and decryption operation times in 1-out-of-n oblivious transfer algorithm. It is not difficult to figure out that using token as the object of oblivious transfers is more effectively than the other.

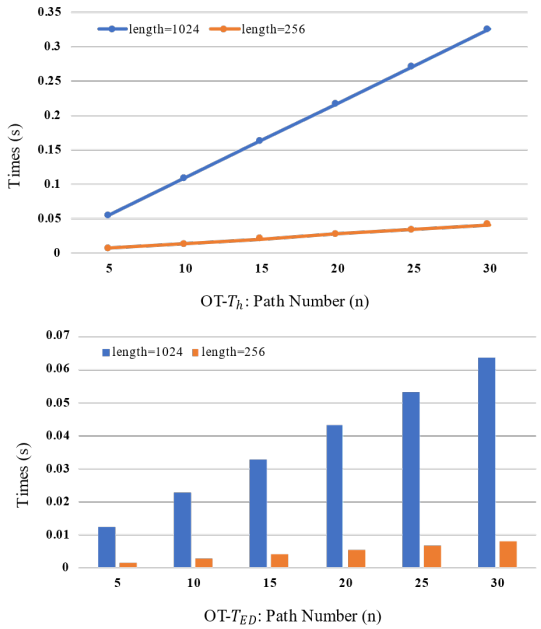

Figure 4. The comparison of computation overhead under 2048-bit string and 256-bit string of data

8 Conclusion

In this paper, a lightweight privacy-preserving path selection scheme in VANETs is proposed, which implements to protect the privacy of users and RSUs. To share n navigation paths to a user, a novel 1-out-of-n oblivious transfers is designed, which ensures the user's request cannot be reveal by RSU and $n - 1$ paths cannot be obtained by user. In addition, a lightweight dual authentication algorithm is proposed to verify the identity between users, RSUs and TAs and resist the replay attack. Moreover, the group key agreement algorithm is provided to support the dynamic group members. The results of performance analysis and evaluation indicate that the proposed scheme has high security and efficiency.

References

[1] H. Hasrouny, E. Samhat, C. Bassil, A. Laouiti, VANet Security Challenges and Solutions: A survey, *Vehicular Communications*, Vol. 7, pp. 7-20, January, 2017.

[2] L. Zhang, B. Kang, F. Dai, Y. Zhang, H. Liu, Hybrid and Hierarchical Aggregation-Verification Scheme for VANET, *IEEE Transactions on Vehicular Technology*, Vol. 71, No. 10, pp. 11189-11200, October, 2022.

[3] G. Sang, J. Chen, Y. Liu, H. Wu, Y. Zhou, S. Jiang, PACM: Privacy-Preserving Authentication Scheme with On-Chain Certificate Management for VANETs, *IEEE Transactions on Network and Service Management*, Vol. 20, No. 1, pp. 216-228, March, 2023.

[4] J. Shen, Z. Gui, X. Chen, J. Zhang, Y. Xiang, Lightweight and Certificateless Multi-Receiver Secure Data Transmission Protocol for Wireless Body Area Networks, *IEEE Transactions on Dependable and Secure Computing*, Vol. 19, No. 3, pp. 1464-1475, May-June, 2022.

[5] O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani, H. Alsariera, A Comprehensive Survey: Benefits, Services, Recent Works, Challenges, Security, and Use Cases for SDN-VANET, *IEEE Access*, Vol. 8, pp. 91028-91047, May, 2020.

[6] X. Zhou, M. Luo, P. Vijayakumar, C. Peng, D. He, Efficient Certificateless Conditional Privacy-Preserving Authentication for VANETs, *IEEE Transactions on Vehicular Technology*, Vol. 71, No. 7, pp. 7863-7875, July, 2022.

[7] C. Lin, X. Huang, D. He, EBCPA: Efficient Blockchain-based Conditional Privacy-preserving Authentication for VANETs, IEEE Transactions on Dependable and Secure Computing, Vol. 20, No. 3, pp. 1818-1832, May-June, 2023.

[8] H. Yang, P. Vijayakumar, J. Shen, B. B. Gupta, A Location-based Privacy-Preserving Oblivious Sharing Scheme for Indoor Navigation, *Future Generation Computer Systems*, Vol. 137, pp. 42-52, December, 2022.

[9] D. Liu, Y. Zhang, W. Wang, K. Dev, S. A. Khowaja, Flexible Data Integrity Checking with Original Data Recovery in IoT-Enabled Maritime Transportation Systems, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 24, No. 2, pp. 2618-2629, February, 2023.

[10] T. Zhou, J. Shen, X. Li, C. Wang, H. Tan, Logarithmic Encryption Scheme for Cyber–Physical Systems Employing Fibonacci Q-matrix, *Future Generation Computer Systems*, Vol. 108, pp. 1307-1313, July, 2020.

[11] J. Shen, H. Yang, P. Vijayakumar, N. Kumar, A Privacy-Preserving and Untraceable Group Data Sharing Scheme in Cloud Computing, *IEEE Transactions on Dependable and Secure Computing*, Vol. 19, No. 4, pp. 2198-2210, July-August, 2022.

[12] M. Bhatnagar, Performance Analysis of a Path Selection Scheme in Multi-Hop Decode-and-Forward Protocol, *IEEE Communications Letters*, Vol. 16, No. 12, pp. 1980-1983, December 2012.

[13] S. D. Ubarhande, D. Doye, S. Nalwade, A Secure Path Selection Scheme for Mobile Ad Hoc Network, *Wireless Personal Communications*, Vol. 97, No. 2, pp. 2087-2096, November, 2017.

[14] P. Xu, Z. Yang, Z. Ding, Z. Zhang, Optimal Relay Selection Schemes for Cooperative NOMA, *IEEE Transactions on Vehicular Technology*, Vol. 67, No. 8, pp. 7851-7855, August, 2018.

[15] S. Khowaja, P. Khuwaja, K. Dev, I. Lee, W. Khan, W. Wang, N. Qureshi, M. Magarini, A Secure Data Sharing Scheme in Community Segmented Vehicular Social

Networks for 6G, *IEEE Transactions on Industrial Informatics*, Vol. 19, No. 1, pp. 890-899, January, 2023.
[16] W. Wang, Z. Han, M. Alazab, T. R. Gadekallu, X. Zhou, C. Su, Ultra Super Fast Authentication Protocol for Electric Vehicle Charging Using Extended Chaotic Maps, *IEEE Transactions on Industry Applications*, Vol. 58, No. 5, pp. 5616-5623, September-October 2022.
[17] X. Wang, X. Kuang, J. Li, J. Li, X. Chen, Z. Liu, Oblivious Transfer for Privacy-Preserving in VANET's Feature Matching, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 22, No. 7, pp. 4359-4366, July, 2021.
[18] V. Yadav, S. Verma, S. Venkatesan, Efficient and Secure Location-based Services Scheme in VANET, *IEEE Transactions on Vehicular Technology*, Vol. 69, No. 11, pp. 13567-13578, November, 2020.
[19] Y. Liang, Y. Liu, B. Gupta, PPRP: Preserving-Privacy Route Planning Scheme in VANETs, *ACM Transactions on Internet Technology*, Vol. 22, No. 4, pp. 1-18, December, 2022.
[20] P. Vijayakumar, M. Azees, A. Kannan, L. J. Deborah, Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 17, No. 4, pp. 1015-1028, April, 2016.
[21] H. Tan, D. Choi, P. Kim, S. Pan, I. Chung, Comments on "Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks", *IEEE Transactions on Intelligent Transportation Systems*, Vol. 19, No. 7, pp. 2149-2151, July, 2018.
[22] R. Vinoth, L. J. Deborah, P. Vijayakumar, N. Kumar, Secure Multifactor Authenticated Key Agreement Scheme for Industrial IoT, *IEEE Internet of Things Journal*, Vol. 8, No. 5, pp. 3801-3811, March, 2021.
[23] H. Tan, W. Zheng, Y. Guan, R. Lu, A Privacy-Preserving Attribute-based Authenticated Key Management Scheme for Accountable Vehicular Communications, *IEEE Transactions on Vehicular Technology*, Vol. 72, No. 3, pp. 3622-3635, March, 2023.
[24] M. Naor, B. Pinkas, Computationally Secure Oblivious Transfer, *Journal of Cryptology*, Vol. 18, No. 1, pp. 1-35, January, 2005.
[25] R. Cramer, V. Shoup, Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption, *International Conference on the Theory and Applications of Cryptographic Techniques*, Amsterdam, The Netherlands, 2002, pp. 45-64.
[26] H. Park, Edge based lightweight Authentication architecture using deep learning for vehicular networks, *Journal of Internet Technology*, Vol. 23, No. 1, pp. 193-200, January, 2022.
[27] H. Cheng, Y. Liu, An Improved RSU-based Authentication Scheme for VANET, *Journal of Internet Technology*, Vol. 21, No. 4, pp. 1137-1150, July, 2020.

Biographies

Guojun Wang recieved a master's degree in software engineering from Nanjing University in 2015, and has been an associate professor of China Yancheng Polytechnic College since 2018. His research interests include cloud computing and security, and information security systems.

Huijie Yang is working toward the Ph.D. degree with Nanjing University of Information Science and Technology. Also, she is currently a visiting Ph.D. student at Singapore Management University, which is supported by the China Scholarship Council under Grant No. 202209040024. Her research interests include security systems, and cryptography.