TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 06/13 pp845–856
DOI: 10.26599/TST.2020.9010043
Volume 26, Number 6, December 2021

EVchain: An Anonymous Blockchain-Based System for Charging–Connected Electric Vehicles

Shiyuan Xu, Xue Chen, and Yunhua He*

Abstract: Purchases of electric vehicles have been increasing in recent years. These vehicles differ from traditional fossil-fuel-based vehicles especially in the time consumed to keep them running. Electric-Vehicle-charging Service Providers (EVSPs) must arrange reasonable charging times for users in advance. Most EVSP services are based on third-party platforms, but reliance on third-party platforms creates a lack of security, leaving users vulnerable to attacks and user-privacy leakages. In this paper, we propose an anonymous blockchain-based system for charging-connected electric vehicles that eliminates third-party platforms through blockchain technology and the establishment of a multi-party security system between electric vehicles and EVSPs. In our proposed system, digital certificates are obtained by completing distributed Public Key Infrastructure (distributed-PKI) identity registration, with the user registration kept separate from the verification process, which eliminates dependence on the EVSP for information security. In the verification process, we adopt smart contracts to solve problems associated with centralized verification and opaque services. Furthermore, we utilize zero-knowledge proof and ring-signature superposition to realize completely anonymous verification, which ensures undeniability and unforgeability with no detriment to anonymity. The evaluation results show that the user anonymity, information authenticity, and system security of our system fulfill the necessary requirements.

Key words: blockchain; Electric Vehicles (EV); zero knowledge proof; distributed Public Key Infrastructure (distributed-PKI); ring signature; smart contract

1 Introduction

With the development of technology in recent years, including parking assistance and smart start-stop technology, smart cars have become increasingly popular[1]. A subclass of the smart car is the Electric Vehicle (EV), which is powered by an electromotor rather than the gasoline of conventional vehicles, which takes relatively little time to fill the tank and requires no advance booking. In contrast, the charging time of the EV is time-consuming, requiring that EV charging Service Providers (EVSPs) be scheduled in advance to arrange a reasonable time for the user vehicles to be charged. So, the establishment of EVSPs is necessary for people who use EVs.

Today, most EVSP systems are based on third-party organizations and rely on a centralized client-server architecture. In this centralized mode, service providers have the authority to access all of the EVs' information, which causes secuirity issues and vulnerability to leakage of private user information. Based on this leaked information, adversaries can infer other information about private users. Today, security and privacy issues are attracting increasing attention[2–5]. Protecting the

• Shiyuan Xu, Xue Chen, and Yunhua He are with the North China University of Technology, Beijing 100144, China. Yunhua He is also with the Beijing Key Laboratory of Internet of Things Security, Institute of Information Engineering, Chinese Academy of Sciences (CAS), Beijing 100093, China. E-mail:13501199447@163.com; chenxuemail0510@163.com; heyunhua@ncut.edu.cn.

∗ To whom correspondence should be addressed.

Manuscript received: 2020-09-03; accepted: 2020-09-23

private information of clients is vital, which is the main problem we resolve in this paper.

The development of a blockchain in distributed ledger architecture provides a viable option. In this paper, we propose an anonymous EV charging system based on blockchain. Our system uses blockchain technology to solve the problem of centralized security via a shared, distributed, tamper-proof, and fault-tolerant database[6, 7]. Smart contracts are used to ensure automation and transparency in the verification process. Examples of the use of blockchain include supply chain management[8]and the Internet of Things (IoTs)[9]. However, blockchain has not been widely used in EVs. Because blockchain can ensure truly distributed security, relevant user information cannot be disclosed to third parties.

Moreover, to ensure the anonymity of our system and make the information even safer, we use hash values during the registration of EV users and the K-anonymity method at the charging station. We also use a distributed Public Key Infrastructure (distributed-PKI), which provides registration legitimacy as an EVSP must collect and store this information. Lastly, we leverage zero-knowledge proof and ring signature technologies to modify EVSP identity to achieve undeniability, unconditional anonymity, and unforgeability.

The contributions of this paper are as follows:

(1) An anonymous blockchain-based system for charging-connected electric vehicles is proposed, in which blockchain technology is used to eliminate the need for trust of and dependence on EVSPs. Using smart contracts, the EV verification process is also automated and transparent.

(2) Privacy protection technologies, such as zero-knowledge proof, ring signature, and K-anonymity, are used to ensure the anonymity and privacy of the EV users in the system.

(3) The feasibility of the system has been verified via security analysis and experimentation.

The rest of this paper is organized as follows: In Section 2, we review related work in EV charging. Current systems and treatment models are discussed in Section 3. In Section 4, we introduce and provide details regarding our system architecture. Evaluations of the anonymity, authenticity, and security of our proposed system are presented in Section 5. Lastly, we draw our conclusions in Section 6.

2 Related Work

2.1 Cryptography privacy approaches in EV charging

In recent years, many researchers have studied ways to preserve the privacy of EV users[10]. To protect both the identity and location of EV users, research in cryptography has included homomorphic encryption, K-anonymity, hash values, and pseudonyms.

Homomorphic encryption is a widely used approach that has also been adopted by some researchers to protect the locations and databases of EV users[11]. This framework can hide user information based on distance calculations. Although this approach can safeguard privacy, total homomorphic encryption of the EV system is required, which is time intensive and limits the capability of other complex functions. Therefore, we choose not to adopt this method for our system.

Many researchers prefer K-anonymity to protect user privacy, which protects the relationship between user-sensitive data and individual identity[12]. This method guarantees that in a set of k similar elements, the target is indiscernible from other $k-1$ elements[13]. Thus, the probability of finding the target user is greatly reduced to $1/k$. Therefore, we use K-anonymity in our system to protect the privacy of the charging information.

Hash values are another cryptology approach used to secure user information. Some scholars consider hash values to be one of the most secure encryption algorithms, and this method is used comprehensively in blockchain systems. Hash values have many characteristics that serve to protect the privacy of users, including strong collision resistance, weak collision resistance, and irreversibility. Furthermore, whatever its input, the output of this method is always 256-bit long. Therefore, it represents a perfect choice in our system.

Pseudonyms have been used extensively for privacy in some cases and were suggested as appropriate for EV users in the IEEE 1609.2 standard[14]. Although this standard is assigned by some trusted third authorities, it only prevents information leakage to untrustworthy parties.

2.2 Zero-knowledge proof

Zero-knowledge proof was proposed by Goldwasser et al.[15] in the late 1980s. It refers to the ability of the prover to convince the verifier that a certain assertion is correct without providing any useful information to the verifier. In the EV charging system, the application of zero-knowledge proof can verify the validity of a transaction without revealing, the user's identity or address, thereby ensuring users privacy and anonymity.

3 Current Systems and Threat Model

In this section, we review some current system models and identify underlying threat models. First, we summarize current EV system models that ignore privacy while incorporating blockchain. Then, we analyze how assailants undermine user privacy in current systems and identify their methods for doing so.

3.1 Current systems

In the current model, the designers do not take privacy into consideration.

As shown in Fig. 1[16], when EVs require charging, EV users must apply to an EVSP. The EVSP then generates a secret function and two keys. The users need to unlock the secret function to verify their identity, and validation process for those who intend to search for charging stations is so weak that users must only input some numbers that are equal to or greater than the original numbers provided. Therefore, if a person inputs some large numbers, he can obtain authentication for any EVs.

Researchers have also considered the security of customer information using the K-anonymity algorithm, but they ignore the fact that the fewer the users, the worse their level of protection[12]. For example, if there are three users, the anonymity set falls to a 3-anonymity set, which means that an adversary has a probability of $p = 1/3$ of accurately determining the others.

Considering these privacy leakage issues, in our system, we utilize distributed-PKI to safeguard security, which we introduce below.

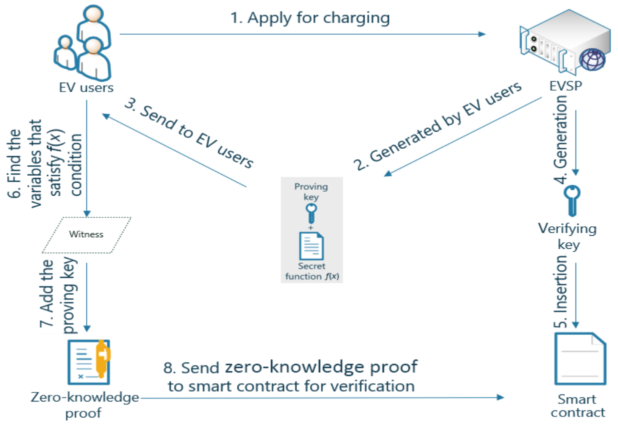

Fig. 1 Current model.

3.2 Basic notions

In our systems, if not specifically mentioned, we use keys 256-bits long and hash functions, and append digital signatures based on the standard digital signature algorithm with Advanced Encryption Standard AES-256 symmetric encryption.

Table 1 lists the basic notations we use in the paper. Three key pairs are used in this paper: $(\mathrm{PK_U}, \mathrm{SK_U})$ is offered via the distributed-PKI systems, $(\mathrm{PK_C}, \mathrm{SK_C})$ is used to generate a zero-knowledge proof Z_{kp}, and $(\mathrm{PK_r}, \mathrm{SK_r})$ represents the key pair of each user in the ring signature. Note that except $(\mathrm{PK_U}, \mathrm{SK_U})$, we do not utilize the Diffie-Hellman (DH) scheme for the public key pairs. Moreover, we let h denote a hash value customized by SHA-256, which is generated in one step. Then, to verify their true identities, we use $\mathrm{sig}_{\mathrm{PK_U}}(\mathrm{PKI})$ as the digital signature for the users, and $\mathrm{Sign_R}$ to represent the ring signature. The three tokens[17] are represented by $T_{\text{v-s}}$, $T_{\text{s-c}}$, and $T_{\text{c-p}}$. Other basic notations are introduced in the following.

3.3 Threat model

Attackers of the current model can obtain an abundance of information, including user behavior patterns, as shown in Table 2.

From Table 2, we can see that "fc1a4...2fd01" always charges at noon, "hae04...9da34" always charges in the afternoon, and "a1830...1b321" often charges at night. Thus, an adversary could deduce EV user habits after a few days.

In addition, the following threats occur frequently in

Table 1 Basic notation.

Notation	Definition
$(\mathrm{PK_U}, \mathrm{SK_U})$	Key pair for registration
h	Hash value of the EV users identity information
Z_{kp}	Zero-knowledge proof
$\mathrm{sig}_{\mathrm{PK_U}}(\mathrm{PKI})$	User's digital signature for PKI
$(\mathrm{PK_C}, \mathrm{SK_C})$	Key pair for zero-kowledge proof
$(\mathrm{PK_r}, \mathrm{SK_r})$	Key pair for ring signature
$\mathrm{Sign_R}$	Signature of zero-knowledge proof
k	Number of members in an anonymous group
$H(x)$	Entropy value
H_{M}	Maximum entropy
p_i	Probability of identifying the i-th individual in the anonymity set with k members
d	Anonymity degree
$T_{\text{v-s}}$	Token used for schedule verification
$T_{\text{s-c}}$	Token used for charge verification
$T_{\text{c-p}}$	Token used for payment verification

Table 2 Information recorded on the blockchain.

$\mathrm{sig}_{\mathrm{PK_U}}$(PKI)	Timestamp of records	Timestamp of validations
fc1a4...2fd01	2020-7-21 11:31	2020-7-21 11:32
fc1a4...2fd01	2020-7-26 11:53	2020-7-26 11:55
hae04...9da34	2020-7-21 14:42	2020-7-21 14:45
hae04...9da34	2020-7-22 15:02	2020-7-22 15:03
hae04...9da34	2020-7-24 14:51	2020-7-24 14:53
hae04...9da34	2020-7-26 15:10	2020-7-26 15:14
a1830...1b321	2020-7-22 22:22	2020-7-22 22:26
a1830...1b321	2020-7-23 22:46	2020-7-23 22:48
a1830...1b321	2020-7-26 23:13	2020-7-26 23:14

decentralized systems (Fig. 2).

(1) EVSP attack

Given that the registration database relies on the EVSP system, we have to assume that if some staff members are not trustworthy, they could become curious about the private information of EV users when scheduling charging services. It is possible for the staff members to view or disclose private user information out of sheer curiosity. This leads to the untrustworthiness of the entire centralized EVSP system.

(2) Man-in-the-middle attack

There may be malicious attackers in systems who can easily capture information from EV scheduling requests received by an EVSP. Having analyzed this information, attackers can then determine user habits and behavior patterns.

(3) Public ledger attack

Blockchain is a publicly distributed ledger in which all system transactions are open and transparent, which enables each node to access any information on the blockchain to quickly reach a consensus. However, when users are authenticated in the blockchain, their private data can be threatened.

(4) Replay attack

To obtain a second charge service, an unethical or malicious user can resubmit authenticated data for repeated authentication.

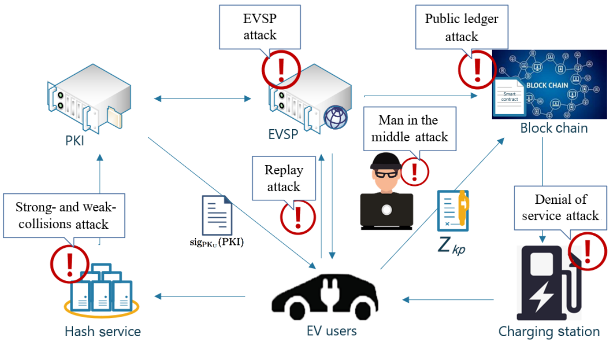

Fig. 2 Attack model for our application.

(5) Denial-of-service attack

The baleful EVs may deliberately take up charging time or an unethical EV may also deliberately take up charging time or occupy a parking space after charging, which can result in subsequently booked vehicles being unable to charge or having insufficient charging time.

(6) Strong- and weak-collisions attack

We must assume that malicious users may try to reverse their anonymous identities. There may also be situations in which the identity certificates of two anonymous users are the same.

4 System Architecture

In this section, we provide an overview of our proposed system and describe the system components in detail.

4.1 System overview

To protect the privacy of EV users, we propose a system that combines hash values and K-anonymity in the registration, with distributed-PKI to verify the true EVSP identity and create a certification for EVs to confirm their identity. In typical circumstances, our system includes three phases: registration, charge scheduling, and charge payment. Figure 3 shows a scheme of this process.

During the registration phase, a user submits a registration application to the distributed-PKI using the hash value of his/her true identity. The distributed-PKI utilizes Registration BlockChain (RBC) and Certificate BlockChain (CBC) node voting to reach a consensus and issue the digital certificate. The EVSP must also register with the distributed-PKI.

In the charge scheduling phase, the user sends a charge request to the EVSP. A pair of $(\mathrm{SK_C}, \mathrm{PK_C})$ is generated when the EVSP receives a request. Then, the user submits a digital certificate, $\mathrm{SK_C}$, and timestamp to generate a zero-knowledge proof Z_{kp}. Three smart contracts are also deployed on the CBC in which the "verify" smart contract is embedded with $\mathrm{PK_C}$. The user then performs a ring signature on the zero-knowledge proof and submits it to the "verify" smart contract for verification. When the user has been authenticated, the EV system will distribute a token to the user as a passport for subsequent actions. Three tokens are used in our system for scheduling, charging, and payment, respectively. These tokens ensure that the scheduling, charging, and payment operations are separate, thereby

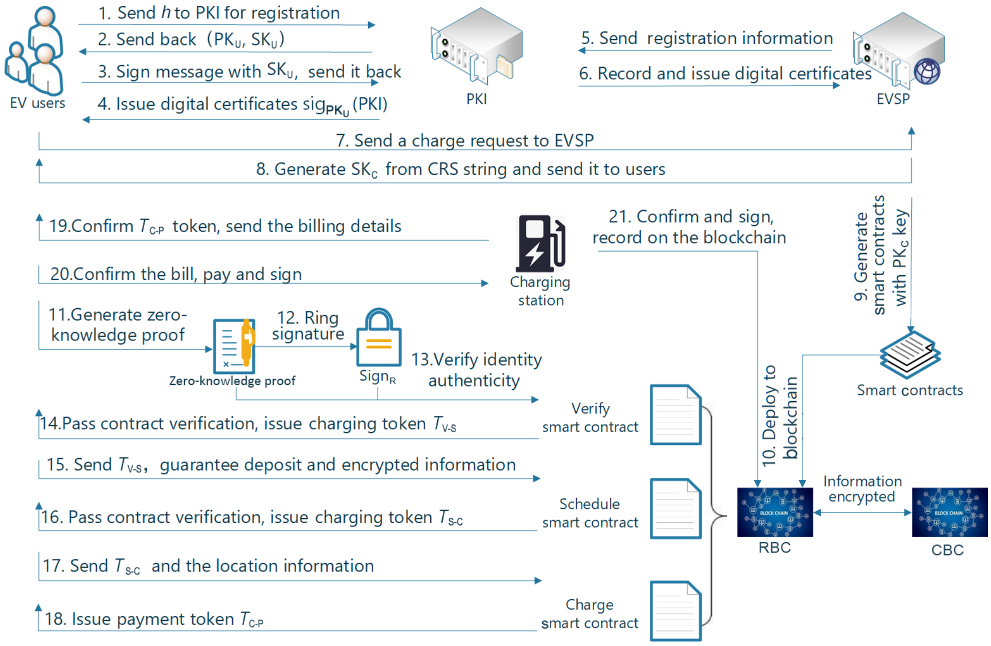
EV users
1. Send h to PKI for registration
2. Send back (PK_U, SK_U)
3. Sign message with SK_U, send it back
4. Issue digital certificates sig_PKU (PKI)
PKI
5. Send registration information
6. Record and issue digital certificates
EVSP
7. Send a charge request to EVSP
8. Generate SK_C from CRS string and send it to users
19.Confirm T_C-P token, send the billing details
20.Confirm the bill, pay and sign
Charging station
21. Confirm and sign, record on the blockchain
9. Generate smart contracts with PK_C key
11.Generate zero-knowledge proof
Zero-knowledge proof
12. Ring signature
Sign_R
13.Verify identity authenticity
Smart contracts
10. Deploy to blockchain
14.Pass contract verification, issue charging token T_V-S
Verify smart contract
15. Send T_V-S, guarantee deposit and encrypted information
16. Pass contract verification, issue charging token T_S-C
Schedule smart contract
Information encrypted
RBC
CBC
17. Send T_S-C and the location information
18. Issue payment token T_C-P
Charge smart contract

Fig. 3 Anonymous blockchain-based system for charging-connected electric vehicles.

protecting the anonymity of the EV user.

If a user identity is verified, a $T_{\text{v-s}}$ token is issued. The user must then submit the encrypted scheduling information, a token $T_{\text{v-s}}$ and a deposit to the "schedule" smart contract. Once verified, EVSP will schedule and issue a $T_{\text{s-c}}$ token to the user. Finally, often when the EV arrives at the charging station, user has to submit the $T_{\text{s-c}}$ token, and RBC verifies its location information. The charging process will begin and a $T_{\text{c-p}}$ token will be issued for payment upon verification.

In the payment phase, the charging station will confirm receipt of the $T_{\text{c-p}}$ token and send a bill to the user. If the user confirms that information is correct, payment will be made using virtual currency and a signature. After the charging station receives payment, the payment must be confirmed and signed, and then recorded on the blockchain.

4.2 Registration

The registration phase is divided into two parts. First, the user registration information is uploaded and cryptography is used to ensure anonymity. Then, a certification for the user is provided using the distributed-PKI method.

PKI is a standard public-key cryptographic management platform that combines user key pairs and a public-key certificate management system to issue certificates. However, traditional PKI is centralized and relies on the security of a third-party certification authority, which may cause security and privacy issues. Therefore, we adopt a distributed-PKI system to complete the registration.

In this phase, the EV user must register his/her ID, payment address, and EV information. In our system, when users apply for registration, we require that they register with a hash value h for the true identity information and generate a digital certificate $\text{sig}_{\text{PK}_\text{U}}$ (PKI) for authentication by two blockchains,

$$h = \text{hashvalue(ID, paymentaddress,}\\ \text{EVinformation)} \quad (1)$$

In this scheme, we utilize some properties of the hash values, such as their uniqueness, unidirectionality, and anti-weak collision, which cannot be used to reverse-decrypt the EV user's real identity. Although a small number of people may know user's true information and obtain their hash value, most of them are family and friends whom we assume to be trustworthy and pose no threat.

We then utilize the K-anonymity algorithm to ensure anonymity, which guarantees that in a set of k similar information, the target information is indistinguishable from other $k-1$ information[13]. Therefore, the probability of finding the real information is $1/k$[18]. The degree of anonymity relies on the member accounts in the anonymity k group. Practically speaking, K-anonymity privacy requires a private server from a trusted third party[18].

After obtaining the hash value for the user's information, we use K-anonymity to ensure the anonymity of our system. To measure the degree of anonymity, information entropy can be proposed to the privacy group, whereby we assume that every individual in the anonymity model of x represents an information point, so we take $H(x)$ to determine its entropy value. Then, we assume Z_{kp} is the possibility of analyzing the i-th member in the anonymity set with k members,

$$H(x) = -\sum_{i=1}^{k} p_{\text{i}} \log_2(p_{\text{i}}) \tag{2}$$

H_{M} is the maximum possible entropy in the K-anonymity set when all k members have the same possibility, i.e., $1/k$, to be searched by other people. Thus, we obtain

$$H_{\text{M}} = \log_2(k) \tag{3}$$

Moreover, the total information that attackers can obtain can be expressed as[19]

$$\frac{H_{\text{M}} - H(x)}{H_{\text{M}}} \tag{4}$$

On this basis, the degree of anonymity is defined by Seys et al.[20] as follows:

$$d = 1 - \frac{H_{\text{M}} - H(x)}{H_{\text{M}}} = \frac{H(x)}{H_{\text{M}}} \tag{5}$$

To verify the user's true identity, we utilize the distributed-PKI method to generate a user certificate. The distributed-PKI consists of RBC, CBC, and EV. After the user has submitted h to the client, the distributed-PKI generates a pair of key $(\text{SK}_{\text{U}}, \text{PK}_{\text{U}})$. The user uses the private key to sign the information and send γ to the RBC,

$$\gamma = \text{Sign}(h, \text{SK}_{\text{U}}) \tag{6}$$

The RBC will vot, and consensus nodes verify v_i,

$$v_i = \text{verify}(\gamma, \text{PK}_{\text{U}}) \tag{7}$$

The client then sends a certificate application to the CBC, which will verify, vote, and generate a digital certificate $(\text{sig}_{\text{PK}_\text{U}}(\text{PKI}))$.

From Fig. 4, we can see that the RBC is used for identification, encryption of the EV identity information, and storage of authenticated EV data. The CBC node is responsible for verification of the validity of the EV, generation of a certificate to authenticate the EV information and EV service information, preservation of undisclosed digital certificates, and maintenance of anonymous digital certificate data. In each blockchain, we use a concurrent Byzantine fault tolerance consensus to assure compatibility, for hard modification of EVs with respect to the nodes, and to protect the consistency of the blockchain[21].

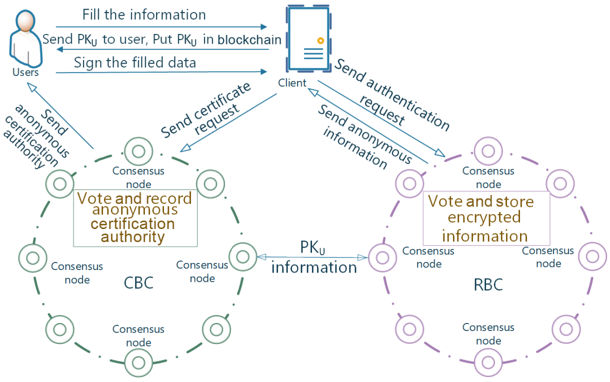
Fill the information
Send PK$_\text{U}$ to user, Put PK$_\text{U}$ in blockchain
Sign the filled data
Users
Client
Send authentication request
Send anonymous information
Send certificate request
Send anonymous certification authority
Consensus node
Vote and record anonymous certification authority
Consensus node
Consensus node
CBC
Consensus node
PK$_\text{U}$ information
Vote and store encrypted information
Consensus node
Consensus node
RBC
Consensus node
Consensus node

Fig. 4 Distributed-PKI system composed of CBC and RBC.

4.3 Charging scheduling

In the charge scheduling phase, we complete three steps: verification, scheduling, and charging of the EV. First, we create the user's zero-knowledge proof and three corresponding smart contracts. Next, we deploy three smart contracts on the blockchain. Lastly, the user enters a ring signature on the zero-knowledge proof and submits it to the smart contracts on the blockchain for verification.

4.3.1 Step 1

When the user desires to charge the EV, he must submit a charge application to the EVSP via the client. Then, the user must submit proof that he/she has already registered. In the registration stage, the user completes the registration of identity in the distributed-PKI and receives a digital certificate $(\text{sig}_{\text{PK}_\text{U}}(\text{PKI}))$. Thus, the user can submit $\text{sig}_{\text{PK}_\text{U}}(\text{PKI})$ to verify his/her identity.

As shown in Fig. 5, the EVSP will distribute a pair of key $(\text{SK}_\text{C}, \text{PK}_\text{C})$ from the Common Reference String (CRS)[22] and send the SK_C to the EV user. Then, the EVSP will create a smart contract with the PK_C. A smart

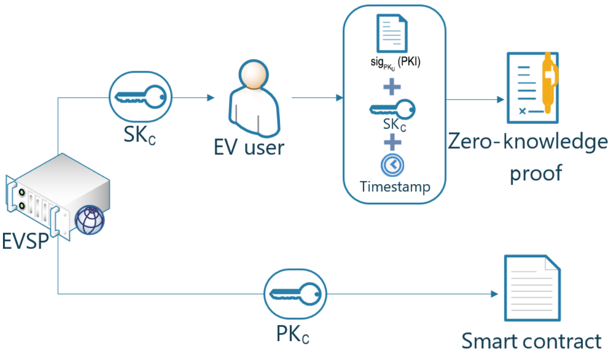

Fig. 5 Step 1: EVSP distributes $(\text{SK}_\text{C}, \text{PK}_\text{C})$ and creates smart contract. Furthermore, the user creates a zero-knowledge proof for subsequent verification.

contract is a computer protocol that propagates, verifies, or informally executes a contract, which is deployed on the blockchain and pre-sets the rules regarding triggered events and responses. Smart contracts are based on reliable and untampered data that automatically execute pre-set rules and respond accordingly. Using "verify" smart contracts in our system serves to decentralize the verification process and make the services more transparent. Lastly, a user utilizes the digital certificate $\text{sig}_{\text{PK}_\text{U}}$(PKI), SK_C, and timestamp together to generate a zero-knowledge proof.

4.3.2 Step 2

In this step, we deploy the "verify", "schedule", and "charge" smart contracts on the CBC when it has been created. To write the smart contracts, we utilize the Zokrates tool and Solidity native language. This operation can be briefly described as consisting of three processes. The first is to perform the secure setup operation to generation the CRS. Next, the zero-knowledge proof is generated using the command generate-proof. Lastly, the export-verifier command is used to export the required smart contract. The PK_C key is embedded in the "verify" smart contract to validate the zero-knowledge proof Z_{kp} of the user. As blockchain is decentralized and distributed, no third party is required to facilitate validation. Thus, we can effectively prevent malicious fraud and data tampering, and resolve the security problem.

4.3.3 Step 3

In the third step, users must ring-sign the zero-knowledge proof. A ring signature is a digital signature scheme originally proposed by Rivest et al.[23]. In this scheme, ring members need not cooperate. The sign verifier only certifies the correctness of the signature without needing to know whose it is. Therefore, the ring signature meets the requirements of correctness, unconditional anonymity, and unforgeability.

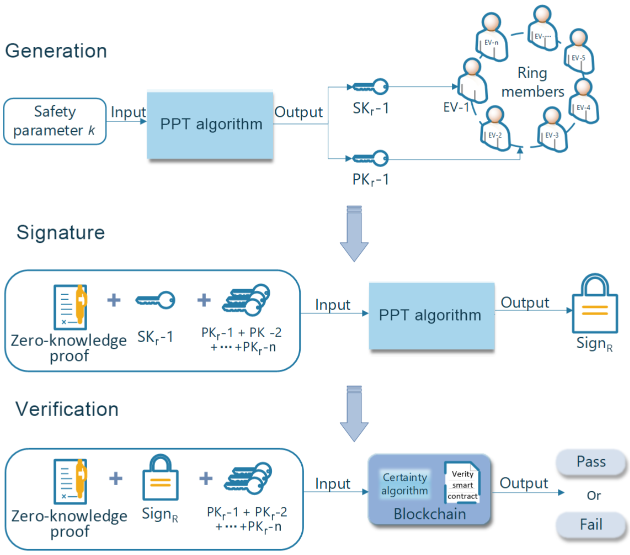

Fig. 6 Three steps of ring signature: generation, signature and verification.

As shown in Fig. 6, first, a key pair is generated for the user by the Probabilistic Polynomial-Time (PPT) algorithm. Next, we enter the user's private keys, zero-knowledge proofs, and the public keys of the ring members for signature. Last, the signature, zero-knowledge proof, and public keys of the ring members are submitted to the "verify" smart contract of the blockchain for verification. The smart contract determines whether the verification should be approved or not. During this process, the user's digital certificate $\text{sig}_{\text{PK}_\text{U}}$(PKI), and timestamp are also approved by the blockchain. Having been successfully authenticated, the "verify" smart contract issues a $T_{\text{v-s}}$ token to the user and stores related information for subsequent scheduling verification.

Next is the scheduling verification process. As shown in Fig. 7, the user submits the $T_{\text{v-s}}$ token, a guarantee deposit, and encrypted scheduling information to the "schedule" smart contract on the blockchain. As the EVSP interacts with smart contracts, it can receive the encrypted scheduling information to schedule an appropriate time slot for the $T_{\text{v-s}}$ token user. After verification, the "schedule" smart contract will withdraw the $T_{\text{v-s}}$ token and return a $T_{\text{s-c}}$ token to the EV to allow it to be charged at a predetermined charging station.

When the EV arrives at the charging station at its designated charging time slot, charging station receives the $T_{\text{s-c}}$ token at its own address. Then, EV charging station verifies the $T_{\text{s-c}}$ token of the EV user to ensure that its identity and schedule are verified. Basically, it uses the token to connect with the "charge" smart contract and receives related identity and schedule information for comparison.

To prevent malicious users from taking this charging slot, we also request the location of the EV vehicle with the identity information. When the user arrives at the charging station, the $T_{\text{s-c}}$ token and location information must be verified. However, user's privacy may be compromised during this process. Therefore, we use a random combination of users at nearby locations in the K-anonymous group to hide the user's personal information. If the verification is approved, the $T_{\text{s-c}}$

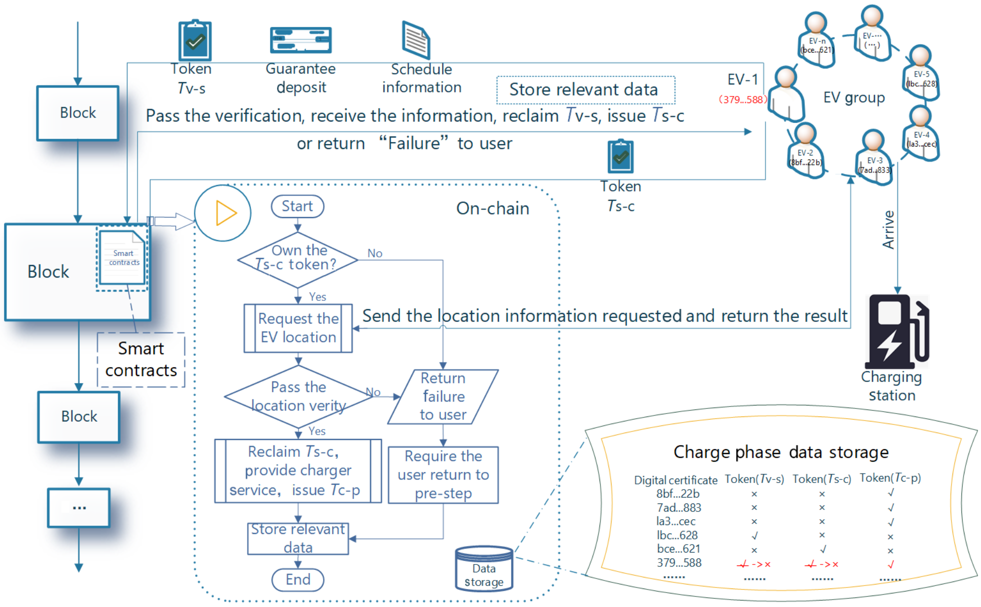

Fig. 7 Step 3: EV user submits required information to the smart contract and verifies it. All relevant informations will be stored on the blockchain.

token is reclaimed and the user is allowed to charge. After charging is complete, a $T_{\text{c-p}}$ token is distributed to the user for subsequent payment, and related information is stored.

4.4 Charging payment

In this section, we describe how the user pays for the electricity used when the EV charging process is complete.

Having charged the EV, the user received a $T_{\text{c-p}}$ token to prove that charging has been completed for payment. The charging station will send its charging time and a unit charging price to the payer, as shown in Fig. 8. After the payer receives the bill, the payment will be made after confirmation. The transaction is recorded in the blockchain to verify the legality of the transaction. The charging station will eventually publish payment information in units of K-anonymous groups to prevent tampering. Users know their own charging time and payment amount, so they can identify their own billing information, but no others can infer details of the hidden information.

5 Evaluation

5.1 Anonymity analysis

In this section, we explain how anonymity is ensured in the EV system. Of primary importance is that the hash value is irreversible, anti-collision, and cannot be cracked. The digital certificate generated by the distributed-PKI provides the user with an identity with the EVSP. When the user wants to charge his/her EV, he/she must submit the zero-knowledge proof to the smart contract, which can perform authentication without providing any private information. Furthermore, the token issued by the smart contract allows users to be verified without submitting any relevant identity information. Last, due to the nature of the K-anonymous group, the probability of an adversary finding the real user is only $1/k$.

In Figs. 9 and 10, we show the time and charging degree of ten groups of users at charging Station A. We can see that the anonymous group is not used in Fig. 9. A malicious attacker can easily analyze the charging habits and vehicle battery capacity of each EV. The users'

00001				$\text{sig}_{\text{PK}_\text{U}}$(PKI)	(EV-1)						
Number field		Pre-work field		Transaction field					Fee payable	Signature	
Num.	Billing number	Deposit($10)	$T_{\text{c-p}}$	Start time	End time	Charging degree	Unit price	Total price	—	Payer	Payee
0	f1x6u7ejhy0msux-0	Yes	Yes	2020-6-26 11:34	2020-6-26 12:59	53	0.4883	$25.9	$15.9	√	√
1	f1x6u7ejhy0msux-1	Yes	Yes	2020-6-29 11:56	2020-6-29 13:13	46	0.4883	$22.5	$12.5	√	√
2	f1x6u7ejhy0msux-2	Yes	No	—	—	—	—	—	—	—	—
...	...	...	...	...	...	...	...	...	...	...	...

Fig. 8 Charging bill details.

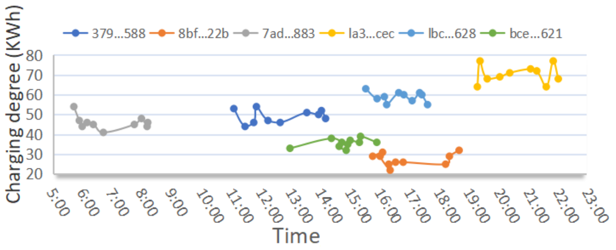

Fig. 9 Charging statistics of Station A before using K-anonymity.

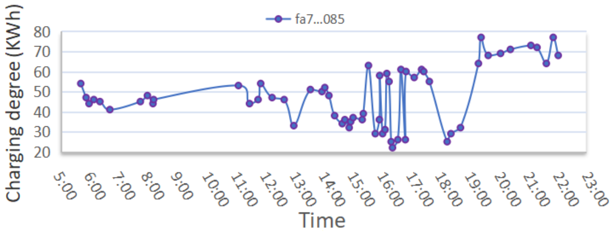

Fig. 10 Charging statistics of Station A after using K-anonymity.

information in Fig. 9 is fully exposed, but in Fig. 10, due to the use of anonymous groups, it is difficult for us to analyze users behavior patterns at a glance, so their personal information remains hidden.

Next, we qualify and evaluate the degree of anonymity of our system for comparison with other systems. To do so, we transform Eq. (5) as follows:

$$d = \frac{H(x)}{H_{\mathrm{M}}} = \frac{-\sum(p_i \times \log_2(p_i))}{-\sum\left(\frac{1}{k} \times \log_2 \frac{1}{k}\right)} = -\frac{\sum(p_i \times \log_2(p_i))}{\log_2(k)} \tag{8}$$

Using the System A[12] as an example, we explain our method for calculating the degree of anonymity as follows: Assuming that there are 10 000 users in the system, each user must re-apply for a pseudonym when every time he/she charges, so each user has 500 pseudonyms to protect their privacy. We assume an EV charge life of 500 charges, so 500 transactions must be recorded for each user on the blockchain. So, the entropy is $H(x) = \log_2(10\,000 \times 500) \approx 22.26$. However, when all users are completely anonymous, the maximum entropy value should be $H_{\mathrm{M}} = \log_2(10\,000 \times 500 \times 500) \approx 30.48$. Therefore, the degree of anonymity of System A in this example is

$$d = \frac{H(x)}{H_{\mathrm{M}}} = \frac{22.26}{30.48} \approx 0.731.$$

As shown in Fig. 11, we evaluated three systems: System A[12], System B[16], and our proposed system. Most existing systems are centralized EVSPs, which can cause user privacy issues. In our system, users use a hash value to register with the distributed-PKI, so there is no need to trust the EVSP. Thus, the anonymity of our system will never be reduced to 0. System A uses pseudonyms and has a trust-based EVSP, so its degree of anonymity is always lower than that of our system. System B, which only uses K-anonymity, is so simple that its degree of anonymity is always lower than both System A and our system.

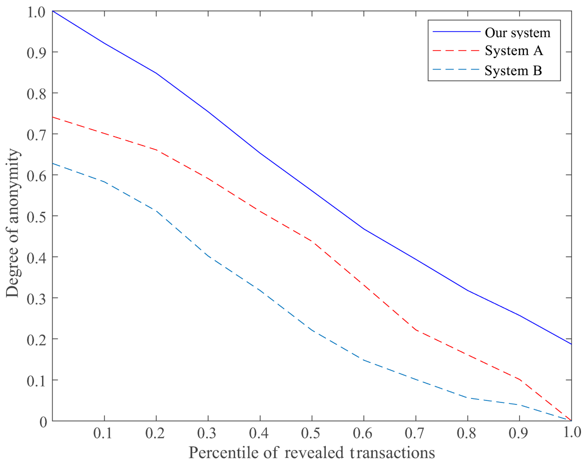

Fig. 11 Degree of anonymity in three systems.

5.2 Authenticity analysis

In addition to anonymity, our system also guarantees authenticity, which is rarely mentioned in other systems. First, a distributed-PKI is specifically used for managing identity registration and certificate generation. In our system, users must register with the distributed-PKI to obtain a digital certificate, which guarantees authenticity of the identity of EV users. Next, we add a timestamp to the zero-knowledge proof generation process to prevent replay attacks. The smart contract verifies the time that the zero-knowledge proof was received. If that time is within the validity period of the proof, the proof is validated, otherwise, it is rejected. We also use ring signatures on the proof to prevent the zero-knowledge proof from being stolen or tampered with.

The process for applying a ring signature is as follows: First, define the function,

$$C_{l,y}(y_1, y_2, y_3, \ldots, y_n) = E_l(y_n \oplus E_l(y_{n-1} \oplus E_l(\cdots y_2 \oplus E_l(y_1 \oplus E_l))) = v_i \tag{9}$$

where E_l is a symmetric encryption algorithm and l is the symmetric key corresponding to E_l.

Use public key PK_{r}-n to encrypt random number x_n, which can be expressed as

$$y_n = g_n(x_n) \tag{10}$$

Use a corresponding private key $\mathrm{SK_r}$-n to decrypt y_n, which can be expressed as

$$x_n = g_n^{-1}(y_n) \tag{11}$$

Taking user EV-1 as an example, we apply a perform ring signature and verify that signature.

The process of generating a ring signature is as follows:

(1) Using the following formula, find E_l and the corresponding symmetric key l,

$$l = \mathrm{hash}(Z_{\mathrm{kp}}) \tag{12}$$

(2) Randomly select a number .

(3) Randomly select $n-1$ values $(x_2, x_3, \ldots, x_n)$, and calculate $(y_2, y_3, \ldots, y_n)$ using Eq. (10).

(4) Find the y_1 value by solving the following equation:

$$C_{l,y}(y_1, y_2, \ldots, y_n) = v \tag{13}$$

(5) Consider y_1 as being encrypted by the public key $\mathrm{PK_r}$-1. As the user has the corresponding private key, x_1 can be obtained by decrypting y_1 by Eq. (11).

(6) Finally, obtain the ring signature E_σ.

$$E_\sigma = (\mathrm{PK_r}\text{-1}, \mathrm{PK_r}\text{-2}, \ldots, \mathrm{PK_r}\text{-n}; v;\ x_1, x_2, \ldots, x_n) \tag{14}$$

The process of verifying the signature is as follows:

(1) The verifier has a public key ($\mathrm{PK_r}$-1, $\mathrm{PK_r}$-2, ..., $\mathrm{PK_r}$-n) and obtains$(y_2, y_3, \ldots, y_n)$ by the encryption of Eq. (10) and the corresponding $(x_1, x_2, \ldots, x_n)$.

(2) Calculate the symmetric key used for E_l by Eq. (12).

(3) Verify Eq. (13). If it is true, it will be approved for verification, otherwise it will be returned.

Using the above signature and verification process, we can see that the ring signature can verify the authenticity of the message by ensuring the anonymity of the user, and the ring signature cannot be forged.

Finally, after the charging is complete, the user will receive a bill from the charging station. After confirming that it is correct, the user will pay and sign. The charging station must also sign after receiving the payment and store it on the blockchain to verify that the bill is true and valid. This evaluation process ensures that the authenticity of our system is better than that of other systems.

5.3 Security analysis

In Section 3.3, a number of threat models were identified, which are resolved by the use of our system:

(1) EVSP attack

We use the storable distributed-PKI system for registration. This information is the only digital certificate generated by the distributed-PKI.

(2) Man-in-the-middle attack

User scheduling information is encrypted and cannot be cracked. In addition, we use the digital certificate issued by the distributed-PKI as the identity and apply K-anonymity to protect user privacy.

(3) Public ledger attack

Attackers can access public ledger information and obtain the user's charging time, charging power, etc. For the following reasons, we believe that this type of attack is impossible in our system:

- A token system is used in our system, and all information is completely encrypted.
- We use K-anonymity to desensitize user information. The probability of identifying a real EV user is only $1/k$.
- When performing charging verification, each user deposits the same amount, and it is impossible to trace information of the same amounts.

(4) Replay attack

A timestamp is added when generating the zero-knowledge proof. Having received the proof, to prevent replay attack, the smart contract on the blockchain will verify whether the current time is within the valid period.

(5) Denial-of-service attack

As each EV user must pay a deposit upon receiving all verifications, it is impossible to forcibly occupy the charging station or to be refused service.

(6) Strong- and weak-collisions attacks

We utilize hash values to resist strong and weak collisions. The hash function maps data of any length to a domain of finite length. The possibility that the hash values of two different data will be the same is extremely small. In addition, it is difficult to identify data based on its hash value.

6 Conclusion

In this paper, we propose a blockchain-based system for charging connected electric vehicles. We utilize distributed-PKI and EVSP, respectively, to provide registration and charge scheduling services. Combining the use of zero-knowledge proof, ring signature, and K-anonymity, we achieve anonymity with respect to user identity and location information. Blockchain smart contracts are also used to ensure service transparency and automatic verification. Our system does not require that a third-party institution, like an EVSP, be trusted. Our evaluation and analysis results confirm that the anonymity, authenticity, and security of the proposed system are guaranteed and exceed those of the current systems.

Acknowledgment

This work was supported by the Natural Science Foundation of Beijing (No. M21029), the National Key Basic R&D Program of China (No. 2018YFB1800302), and the National Natural Science Foundation of China (No. 61802005).

References

[1] A. G. Bianchessi, C. Ongini, I. Boniolo, G. Alli, C. Spelta, M. Tanelli, and S. M. Savaresi, A novel electric vehicle for smart indoor mobility, *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 4, pp. 1429–1440, 2014.

[2] Y. Wu, Y. Lyu, and Y. Shi, Cloud storage security assessment through equilibrium analysis, *Tsinghua Science and Technology*, vol. 24, no. 6, pp. 738–749, 2019.

[3] J. Liu, Y. Yu, J. Jia, S. Wang, F. P. Fan, H. Wang, and H. Zhang, Lattice-based double-authentication-preventing ring signature for security and privacy in vehicular ad-hoc networks, *Tsinghua Science and Technology*, vol. 24, no. 5, pp. 575–584, 2019.

[4] Y. Khazbak, J. Fan, S. Zhu, and G. Cao, Preserving personalized location privacy in ride-hailing service, *Tsinghua Science and Technology*, vol. 25, no. 6, pp. 743–557, 2020.

[5] S. Liang, Y. Zhang, B. Li, X. Guo, C. Jia, and Z. Liu, SecureWeb: Protecting sensitive information through the web browser extension with a security token, *Tsinghua Science and Technology*, vol. 23, no. 5, pp. 526–538, 2018.

[6] D. Kundur and D. Hatzinakos, Digital watermarking for telltale tamper proofing and authentication, *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1167–1180, 1999.

[7] D. Tosh, S. Sengupta, C. A. Kamhoua, and K. A. Kwiat, Establishing evolutionary game models for CYBer security information EXchange (CYBEX), doi: 10.1016/j.jcss.2016.08.005.

[8] V. Naidu, K. Mudliar, A. Naik, and P. P. Bhavathankar, A fully observable supply chain management system using block chain and IoT, in *Proc. of 2018 3rd International Conference for Convergence in Technology*, Pune, India, 2018.

[9] Y. Liu, K. Wang, K. Qian, M. Du, and S. Guo, Tornado: Enabling blockchain in heterogeneous internet of things through a space-structured approach, *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 1273–1286, 2020.

[10] D. Gabay, K. Akkaya, and M. Cebe, Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs, *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5760–5772, 2020.

[11] C. Zhang, L. Zhu, J. Ni, C. Huang, and X. Shen, Verifiable and privacy-preserving traffic flow statistics for advanced traffic management systems, *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 10 336–10 347, 2020.

[12] M. D. Firoozjaei, A. Ghorbani, H. Kim, and J. SongFiroozjaei, EVChain: A blockchain-based credit sharing in electric vehicles charging, in *Proc. of 2019 17th International Conference on Privacy, Security and Trust*, Fredericton, Canada, 2019, pp. 1–5.

[13] A. Machanavajjhala, D. Kifer, and J. Gehrke, L-diversity: Privacy beyond K-anonymity, *ACM Transactions on Knowledge Discovery from Data*, vol. 1, no. 1, p. 3, 2007.

[14] H. Li, G. Dan, and K. Nahrstedt, Portunes: Privacy-preserving fast authentication for dynamic electric vehicle charging, in *Proc. of 2014 IEEE International Conference on Smart Grid Communications* (*SmartGridComm*), Venice, Italy, 2014, pp. 920–925.

[15] S. Goldwasser, S. Micali, and C. Rackoff, The knowledge complexity of interactive proof systems, *SIAM Journal on Computing*, doi: 10.1137/0218012, 1989.

[16] D. Gabay, K. Akkaya, and M. Cebe, A privacy framework for charging connected electric vehicles using blockchain and zero knowledge proofs, in *Proc. of 2019 IEEE 44th LCN Symposium on Emerging Topics in Networking* (*LCN Symposium*), Osnabrück, Germany, 2019, pp. 64–73.

[17] R. Rahimian, S. Eskandari, and J. Clark, Resolving the multiple withdrawal attack on ERC20 tokens, in *Proc. of 2019 IEEE European Symposium on Security and Privacy Workshops*, Stockholm, Sweden, 2019, pp. 320–329.

[18] P. Samarati and L. Sweeney, Generalizing data to provide anonymity when disclosing information (abstract), in *Proc. of 1998 17th ACM SIGACTSIGMOD-SIGART Symposium on Principles of Database Systems*, Seattle, WA, USA, 1998, p. 188.

[19] M. D. Firoozjaei, J. Yu, H. Choi, and H. Kim, Privacy-preserving nearest neighbor queries using geographical features of cellular networks, *Computer Communications*, vol. 98, pp. 11–19, 2017.

[20] S. Seys, J. Claessens, and B. PreneelDiaz, Towards measuring anonymity, in *Proc. of 2nd International Conference on Privacy Enhancing Technologies*, San Francisco, CA, USA, 2003, pp. 54–68.

[21] W. Hu, Y. Hu, W. Yao, and H. Li, A Blockchain-based byzantine consensus algorithm for information authentication of the internet of vehicles, *IEEE Access*, vol. 7, pp. 139 703–139 711, 2019.

[22] J. Eberhardt and S. Tai, ZoKrates-scalable privacy-preserving off-chain computations, in *Proc. of 2018 IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data*, Halifax, Canada, 2018, pp. 1084–1091.

[23] R. L. Rivest, A. Shamir, and Y. Tauman, How to leak a secret, in *Proc. of 2001 International Conference on the Theory and Application of Cryptology and Information Security*, Daejeon, Korea, 2001, pp. 552–565.

Shiyuan Xu is an undergraduate student at the North China University of Technology. His research interests include post-quantum cryptography, security, and privacy in vehicle ad hoc networks. He has published several articles in refereed international conferences and journals.

Xue Chen is an undergraduate student at the North China University of Technology. She has published several articles in refereed international conferences and journals. Her research interests include post-quantum cryptography, blockcain, and privacy and security in vehicle ad hoc networks.

Yunhua He received the PhD degree in computer science from Xidian University, Xi'an, China in 2016. He is an assistant professor at the North China University of Technology. His research interests include security and privacy in cyber-physical systems, bitcoin-based incentive mechanism, security, and privacy in vehicle ad hoc networks. He has published 20 research articles in refereed international conferences and premier journals. He received the Best Paper Award from the conference WASA 2017.