

Security and Privacy Preservation in Blockchain-Based Intelligent Transportation Systems

Lead Guest Editor: Haowen Tan

Guest Editors: Ilyong Chung and Shichang Xuan





Security and Privacy Preservation in Blockchain-Based Intelligent Transportation Systems

Security and Communication Networks

**Security and Privacy Preservation
in Blockchain-Based Intelligent
Transportation Systems**

Lead Guest Editor: Haowen Tan

Guest Editors: Ilyong Chung and Shichang Xuan






Copyright © 2022 Hindawi Limited. All rights reserved.

This is a special issue published in "Security and Communication Networks." All articles are open access articles distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Chief Editor

Roberto Di Pietro, Saudi Arabia

Associate Editors

Jiankun Hu , Australia
Emanuele Maiorana , Italy
David Megias , Spain
Zheng Yan , China

Academic Editors



Saed Saleh Al Rabae , United Arab Emirates
Shadab Alam, Saudi Arabia
Goutham Reddy Alavalapati , USA
Jehad Ali , Republic of Korea
Jehad Ali, Saint Vincent and the Grenadines
Benjamin Aziz , United Kingdom
Taimur Bakhshi , United Kingdom
Spiridon Bakiras , Qatar
Musa Balta, Turkey
Jin Wook Byun , Republic of Korea
Bruno Carpentieri , Italy
Luigi Catuogno , Italy
Ricardo Chaves , Portugal
Chien-Ming Chen , China
Tom Chen , United Kingdom
Stelvio Cimato , Italy
Vincenzo Conti , Italy
Luigi Coppolino , Italy
Salvatore D'Antonio , Italy
Juhriyansyah Dalle, Indonesia
Alfredo De Santis, Italy
Angel M. Del Rey , Spain
Roberto Di Pietro , France
Wenxiu Ding , China
Nicola Dragoni , Denmark
Wei Feng , China
Carmen Fernandez-Gago, Spain
AnMin Fu , China
Clemente Galdi , Italy
Dimitrios Geneiatakis , Italy
Muhammad A. Gondal , Oman
Francesco Gringoli , Italy
Biao Han , China
Jinguang Han , China
Khizar Hayat, Oman
Azeem Irshad, Pakistan

M.A. Jabbar , India
Minho Jo , Republic of Korea
Arijit Karati , Taiwan
ASM Kayes , Australia
Farrukh Aslam Khan , Saudi Arabia
Fazlullah Khan , Pakistan
Kiseon Kim , Republic of Korea
Mehmet Zeki Konyar, Turkey
Sanjeev Kumar, USA
Hyun Kwon, Republic of Korea
Maryline Laurent , France
Jegatha Deborah Lazarus , India
Huaizhi Li , USA
Jiguo Li , China
Xueqin Liang, Finland
Zhe Liu, Canada
Guangchi Liu , USA
Flavio Lombardi , Italy
Yang Lu, China
Vincente Martin, Spain
Weizhi Meng , Denmark
Andrea Michienzi , Italy
Laura Mongioi , Italy
Raul Monroy , Mexico
Naghme Moradpoor , United Kingdom
Leonardo Mostarda , Italy
Mohamed Nassar , Lebanon
Qiang Ni, United Kingdom
Mahmood Niazi , Saudi Arabia
Vincent O. Nyangaresi, Kenya
Lu Ou , China
Hyun-A Park, Republic of Korea
A. Peinado , Spain
Gerardo Pelosi , Italy
Gregorio Martinez Perez , Spain
Pedro Peris-Lopez , Spain
Carla Ràfols, Germany
Francesco Regazzoni, Switzerland
Abdalhossein Rezai , Iran
Helena Rifà-Pous , Spain
Arun Kumar Sangaiah, India
Nadeem Sarwar, Pakistan
Neetesh Saxena, United Kingdom
Savio Sciancalepore , The Netherlands

De Rosal Ignatius Moses Setiadi ,
Indonesia
Wenbo Shi, China
Ghanshyam Singh , South Africa
Vasco Soares, Portugal
Salvatore Sorce , Italy
Abdulhamit Subasi, Saudi Arabia
Zhiyuan Tan , United Kingdom
Keke Tang , China
Je Sen Teh , Australia
Bohui Wang, China
Guojun Wang, China
Jinwei Wang , China
Qichun Wang , China
Hu Xiong , China
Chang Xu , China
Xuehu Yan , China
Anjia Yang , China
Jiachen Yang , China
Yu Yao , China
Yinghui Ye, China
Kuo-Hui Yeh , Taiwan
Yong Yu , China
Xiaohui Yuan , USA
Sherali Zeadally, USA
Leo Y. Zhang, Australia
Tao Zhang, China
Youwen Zhu , China
Zhengyu Zhu , China


Contents

A New Code-Based Traceable Ring Signature Scheme

Yanhong Qi  and Li-Ping Wang 

Research Article (10 pages), Article ID 3938321, Volume 2022 (2022)

A Summary of Security Techniques-Based Blockchain in IoV

Chen Chen and Shi Quan 

Review Article (14 pages), Article ID 8689651, Volume 2022 (2022)

Threshold Key Management Scheme for Blockchain-Based Intelligent Transportation Systems

Tianqi Zhou , Jian Shen , Yongjun Ren , and Sai Ji 

Research Article (8 pages), Article ID 1864514, Volume 2021 (2021)

Research Article

A New Code-Based Traceable Ring Signature Scheme

Yanhong Qi ^{1,2} and Li-Ping Wang ^{1,2}

¹State Key Laboratory of Information Security, Institute of Information Engineering, CAS, Beijing, China

²School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China

Correspondence should be addressed to Li-Ping Wang; wangliping@iie.ac.cn

Received 19 November 2021; Revised 29 January 2022; Accepted 10 March 2022; Published 29 April 2022

Academic Editor: Shichang Xuan

Copyright © 2022 Yanhong Qi and Li-Ping Wang. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Traceable ring signatures (TRS) can reveal the identity of the signer if he signs two different messages on the same tag in the group of users. They are widely used in e-voting and cryptocurrencies such as Monero. However, there is still no secure code-based TRS scheme in the random oracle model (ROM). In this paper, we propose a code-based TRS scheme whose security is based on the hardness of the syndrome decoding problem and 2-regular null syndrome decoding problem. We show that our scheme is secure in the ROM in terms of tag-linkability, anonymity, and culpability. The signature size of our scheme is logarithmic in terms of the ring size.

1. Introduction

Ring signatures can be regarded as special group signatures, but they are differing from group signatures in that there is no group administrator in ring signatures. So, we cannot trace the real identity of the signer like group signatures. Ring signatures allow users from a group to sign messages on behalf of the group. The verifier of the ring signature can check the correctness of the signature but cannot know which person in the group is the real signer. If the same signer generates two signatures, the verifier cannot identify the signer. However, in many application scenarios [1–4], the signature represents the use by the signer of his rights, so it is important to be able to trace the signer who signs twice. For example, in a voting system for an event, users in the group can anonymously vote for the event. Dishonest users can use anonymity to vote multiple times for their own benefit. Therefore, in this case, a verifier wants to track the identities of dishonest users while protecting the privacy of honest users.

In order to solve this problem, the first traceable ring signature (TRS) scheme was proposed by Fujisaki and Suzuki [5]. TRS schemes have many applications in e-voting and cryptocurrencies such as Monero. A TRS scheme can track the dishonest's information while protecting the

privacy of honest users. A TRS scheme has a tag that contains public keys of the group members and an issue. For example, an issue may be an election or a social problem. Group members can post any signed and anonymous opinions on the issue only once per tag. If a member wants to support his first opinion and submits another signed opinion, his identity will be immediately revealed. More specifically, if the signer signs the same message twice with the same tag, one will see that the two signatures are linked. If the signer signs different messages with the same tag, a TRS scheme can not only prove that the two signatures are related but also expose the identity of the signer.

There are many TRS schemes [1–3, 6–8] based on factoring and discrete logarithm problems. With the emergence of large-scale quantum computers, most classic asymmetric cryptography is threatened because Shor's algorithm can solve factoring and discrete logarithm problems in polynomial times [9]. Therefore, the postquantum secure TRS schemes have attracted much attention. Branco and Mateus proposed the first post-quantum TRS scheme which is based on coding theory [10]. However, the TRS was pointed out to be unsafe due to the use of the Cramer-Damgård-Schoenmakers (CDS) framework [11] to construct OR relation in [12]. The authors in [12] also proposed a general framework and instantiated the framework with lattice-

based building blocks. A hash-based one-time traceable ring signature was proposed in [13]. [14] was an extension of the work in [12]. In [14], not only lattice-based instantiation of the framework was given but also the instantiation based on symmetric-key primitives. Unlike the framework proposed in [14], we use a different way to construct the signing process and the detailed information is described in III.

Code-based cryptography is a hot topic because it is thought to be secure against attacks by quantum computers. The first code-based signature scheme appeared in 2001 [15]. And then, code-based signature schemes have developed greatly in the last years [16–18]. The first code-based ring signature was proposed in 2007 [19]. After that, many variations related to ring signatures have been proposed, such as linkable ring signature schemes [20], threshold ring signature schemes [21–23], and group signature schemes [24–28]. However, there is still no secure code-based TRS scheme in the random oracle model (ROM).

Our Contributions. In this paper, we propose a new code-based TRS scheme in the ROM. Our scheme is an improvement on [10]. Instead of using the CDS framework in [10], we employ an accumulator [29] to construct the OR relation. Our scheme is based on the syndrome decoding (SD) problem and 2-regular null syndrome decoding (2-RNSD) problem, and we give the security analysis of the scheme in the ROM. More precisely, we construct a new protocol called Acc-GStern’s protocol by adding new relationships to the GStern’s protocol [10]. The GStern’s protocol is for a prover to prove that he has the knowledge of an error vector \mathbf{e} for two instances of the SD problem. The Acc-GStern’s protocol is for one prover to prove that not only does he have the knowledge of a witness \mathbf{e} for one of the several instances of the general syndrome decoding (GSD) problem but also he has values that can correctly be accumulated into the root of the code-based Merkle-tree.

Consider members in the ring. For $1 \leq i \leq L$, let $(\mathbf{H}, \mathbf{s}_i)$ be the public keys of each user \mathcal{P}_i , and the corresponding private key is \mathbf{e}_i . To sign a message, \mathcal{P}_i collects the public keys of remaining $L - 1$ members in the ring and uses them to get a hash value \tilde{H} . Then, \mathcal{P}_i uses his secret key to get a vector $\mathbf{r}_i = \tilde{H}\mathbf{e}_i^T$ and adds a hash function on \mathbf{r}_i to get. Next, the user uses a special hash function [29] to get the leaves of the Merkle-tree and applies the Fiat-Shamir transform [30] on the Acc-GStern’s protocol to get the signature. If the signer signs two different messages in the same ring, the identity of the signer is revealed.

The remainder of this paper is as follows: Section 2 introduces the necessary preliminary knowledge needed in this paper. In Section 3, we present our TRS scheme. The security proof and analysis of the scheme are given in Section 4. Efficiency is shown in Section 5. Finally, the conclusion is drawn in Section 6.

2. Preliminaries

2.1. Notations. Let us start with some notations. We write \mathbb{Z}_2 as the set $\{0, 1\}$ and use $[n]$ to denote the set. We use $(\mathbf{r}_i)_{i \in [L]}$ to represent the sequence $(\mathbf{r}_1, \mathbf{r}_2, \dots, \mathbf{r}_L)$. Vectors and matrices will be represented in boldface lowercase letters and bold capital letters, respectively. If S is a finite set, it means

that y is chosen uniformly at random from S . If \mathcal{A} is an algorithm, we use $y \leftarrow \mathcal{A}(x)$ to show that when running with input x , the output of this algorithm is y . Let $w(\mathbf{y})$ be the Hamming weight of the vector \mathbf{y} . We represent the transpose of \mathbf{b} in terms of \mathbf{b}^T . The bit-wise addition operation modulo 2 is denoted by \oplus . The function A which is negligible under the parameter n is denoted by $\text{negl}(n)$, i.e., $A \leq 1/\text{poly}(n)$, where $\text{poly}(n)$ represents any polynomial in n .

2.2. Hard Problems. In this section, we are going to cover some of the difficult problems used later.

Problem 1 (syndrome decoding (SD) problem). Let $\mathbf{H} \in \{0, 1\}^{(n-k) \times n}$ be a parity-check matrix of an $[n, k]$ random linear code, $\mathbf{s} \in \{0, 1\}^{n-k}$ be a binary vector, $t \geq 0$ be an integer, find $\mathbf{e} \in \mathbb{Z}_2^n$ such that $w(\mathbf{e}) \leq t$, and $\mathbf{H}\mathbf{e}^T = \mathbf{s}^T$.

This problem is proven to be NP-complete in the worst case [31]. The distance between the uniform distribution over $\mathbb{Z}_2^{(n-k) \times n} \times \mathbb{Z}_2^{n-k}$ and $(\mathbf{H}, \mathbf{H}\mathbf{e}^T)$ is negligible [25].

Lemma 1 (see [10]). Let $n, k' \in \mathbb{Z}$, and $k' \leq n/2$. Let \mathbf{H} be a random matrix in $\mathbb{Z}_2^{k' \times n}$ and \mathbf{s} be a random vector in $\mathbb{Z}_2^{k'}$. The probability that one can find \mathbf{e} that satisfies $\mathbf{H}\mathbf{e}^T = \mathbf{s}^T$ is negligible.

Problem 2 (general syndrome decoding (GSD) problem). Let $\mathbf{H}, \mathbf{G} \in \{0, 1\}^{(n-k) \times n}$ be binary matrices, \mathbf{s}, \mathbf{r} be binary vectors, and $t \geq 0$ be an integer. The problem is to find $\mathbf{e} \in \mathbb{Z}_2^n$ such that $w(\mathbf{e}) \leq t$ and $\mathbf{H}\mathbf{e}^T = \mathbf{s}^T, \mathbf{G}\mathbf{e}^T = \mathbf{r}^T$.

The RSD problem is also proved to be NP-complete since the SD problem can be trivially reduced to the GSD problem [10].

Lemma 2. Let $n, k' \in \mathbb{Z}$, and $k' \leq n/4$. Let $\mathbf{H}, \mathbf{G} \in \{0, 1\}^{(n-k) \times n}$ be two random matrices in $\mathbb{Z}_2^{k' \times n}$ and \mathbf{s}, \mathbf{r} be two random vectors in $\mathbb{Z}_2^{k'}$. The probability that one can find \mathbf{e} that satisfies (HTML translation failed) and $\mathbf{G}\mathbf{e}^T = \mathbf{r}^T$ is negligible.

Definition 1 (see [32]). A regular word is a vector of length n and weight w , and it has exactly one nonzero position in each w intervals $[(i-1)n/w; in/w]_{i=1, \dots, w}$. Furthermore, if the weight of each interval is two or zero, the word is called 2-regular. A 2-regular word is the sum of two regular words.

Problem 3 (2-regular null syndrome decoding (2-RNSD) problem). Let $n, k, c, m \in \mathbb{Z}$, and $m = 2^c \cdot k/c$. Let $\mathbf{B} \in \mathbb{Z}_2^{n \times m}$ be a randomly matrix. The problem is to find a nonzero 2-regular word \mathbf{z} such that $\mathbf{B} \cdot \mathbf{z} = 0$.

This problem turns out to be NP hard in the worst case [32].

Definition 2 (see [33]). For any probabilistic polynomial time adversary \mathcal{A} , a collision-resistant hash function h satisfies

$$\Pr[(\mathbf{x}, \mathbf{x}') \leftarrow \mathcal{A}(1^\lambda, h): \mathbf{x} \neq \mathbf{x}', h(\mathbf{x}) = h(\mathbf{x}')] \leq \rho(\nu),$$

where $\rho(\nu)$ is a negligible function.

Definition 3 (see [14]). A noninteractive protocol $\Pi = (\text{Setup}, \mathcal{P}, \mathcal{V})$ for a relation R is zero-knowledge, if there

exists a pair of PPT algorithms called simulator (S_O, S_P) s.t. for every PPT adversary \mathcal{A} , we have that

$$\begin{aligned} & |\Pr[b = 1: pp \leftarrow \mathbf{Setup}(1^\lambda), b \leftarrow \mathcal{A}^{\mathcal{O}_1(pp, \cdot)}(pp)] \\ & - \Pr[b = 1: (pp, \zeta) \leftarrow S_O(1^\lambda), b \leftarrow \mathcal{A}^{\mathcal{O}_2(pp, \zeta)}(pp)]| \quad (1) \\ & \leq \text{negl}(\lambda), \end{aligned}$$

where \mathcal{O}_1 and \mathcal{O}_2 first validate that the input $(x, w) \in R$, else return \perp ; otherwise, \mathcal{O}_1 outputs $\pi \leftarrow \mathcal{P}_i$, and \mathcal{O}_2 outputs $\pi \leftarrow S_P$.

2.3. Merkle-Tree-Based Accumulator. In this section, we first introduce a Merkle-tree-based accumulator scheme [29] which is a building block of our traceable ring scheme. The accumulator is a one-way membership function that takes a set R as input and outputs a constant size value \mathbf{u} . At the same time, a value $\mathbf{d} \in R$ has a short witness \mathbf{w} , which makes the verifier believe that \mathbf{d} was accumulated to \mathbf{u} . The accumulator based on Merkle-tree structure is efficient and is also based on the following code-based hash function \mathcal{H} .

Definition 4 (see [29]). Let $m = 2 \cdot 2^c \cdot n/c$, $\text{RE}: \{0, 1\}^n \rightarrow \{0, 1\}^{2^c \cdot n/c}$ be an encoding function that maps \mathbf{x} to (HTML translation failed). Consider a random matrix $\mathbf{B} = [\mathbf{B}_0 | \mathbf{B}_1]$, where $\mathbf{B}_0, \mathbf{B}_1 \in \mathbb{Z}_2^{n \times m/2}$. The hash function $\mathcal{H} = \{h_{\mathbf{B}} | \mathbf{B} \in \mathbb{Z}_2^{n \times m}\}$ mapping $\{0, 1\}^n \times \{0, 1\}^n$ to $\{0, 1\}^n$ is defined as

$$h_{\mathbf{B}}(\mathbf{u}_0, \mathbf{u}_1) = \mathbf{B}_0 \cdot \text{RE}(\mathbf{u}_0) \oplus \mathbf{B}_1 \cdot \text{RE}(\mathbf{u}_1). \quad (2)$$

Lemma 3 (see [29]). The above function family \mathcal{H} is collision-resistant if the 2-RNSD problem is hard.

The accumulator scheme consists of four algorithms:

- (1) **Setup** (λ) : the input is public parameters (pp) . The output is a key \mathbf{B} for the hash function.
- (2) **Accu** $_{\mathbf{B}}(R = \{\mathbf{d}_0, \dots, \mathbf{d}_{N-1}\} \subseteq (\{0, 1\}^n)^N)$: the input is all the elements in R that treats each element as a leaf node of the Merkle-tree. The output is the root note \mathbf{u} , which is also called the accumulated value, accumulating by R .
- (3) **WitGen** $_{\mathbf{B}}(R, \mathbf{d})$: the input is \mathbf{d} . If $\mathbf{d} \in R$, the output is the witness w for \mathbf{d} . Otherwise, the output is \perp .
- (4) **Verify** $_{\mathbf{B}}(\mathbf{u}, \mathbf{d}, w)$: the inputs are \mathbf{u}, \mathbf{d} , and w . In order to obtain the accumulate value \mathbf{u} , the verifier checks whether w is the valid hash path of \mathbf{u} .

2.4. Traceable Ring Signatures. In this section, we give the definition and security model of traceable ring signatures. For simplicity of discussion, we denote $\overline{pk} = (\text{pk}_1, \dots, \text{pk}_L)$, where pk_i is the public key of each user in the ring. Let issue be a string that represents the target of the signature (for example, a transaction or an election).

2.4.1. Syntax. A TRS scheme contains four polynomial time algorithms defined as follows.

- (i) $(\text{pk}, \text{sk}) \leftarrow \mathbf{KeyGen}(1^\lambda)$: the input is the security parameter λ . **KeyGen** generates public and secret parameters and outputs the pair of public and secret key (pk, sk) .
- (ii) $\sigma \leftarrow \mathbf{Sign}(\text{sk}_i, T, M)$: the inputs are the secret sk_i of the user \mathcal{P}_i , a tag $T := (\overline{pk}, \text{issue})$, and a message $M \in \{0, 1\}^*$. The output is a signature σ on message M with the tag T . The \overline{pk} contains all the members in the ring and pk_i should be in \overline{pk} .
- (iii) $b \leftarrow \mathbf{Ver}(T, M, \sigma)$: the inputs are the tag $T = (\overline{pk}, \text{issue})$, the signature σ , and the message M . The output is $b = 1$ if accepting the signature or $b = 0$ if not accepting it.
- (iv) $s \leftarrow \mathbf{Trace}(T, M_1, M_2, \sigma_1, \sigma_2)$: the inputs are the tag T and two message/signature pairs $(M_1, \sigma_1), (M_2, \sigma_2)$ that correspond to private keys sk_i and sk_j , respectively. If $\mathbf{Ver}(T, \sigma_1, M_1) = 1$ and $\mathbf{Ver}(T, \sigma_2, M_2) = 1$, the output is s , that is either equal to linked, accept, or pk_i :

$$\mathbf{Trace}(T, M_1, M_2, \sigma_1, \sigma_2) := \begin{cases} \text{accept,} & \text{if } i \neq j, \\ \text{linked,} & \text{else if } M_1 = M_2, \\ \text{pk}_i, & \text{otherwise } (M_1 \neq M_2). \end{cases} \quad (3)$$

The correctness conditions of TRS are completeness and public traceability. The definitions are given as follows:

Definition 5 (completeness). Let $i \in [L]$ and $T := (\overline{pk}, \text{issue})$ for some issues. If for all $(\text{pk}, \text{sk}) \leftarrow \mathbf{KeyGen}(1^\lambda), \sigma \leftarrow \mathbf{Sign}(\text{sk}_i, T, M)$ and all M , it holds that $\mathbf{Ver}(T, M, \sigma) = 1$.

Definition 6 (public traceability). A TRS satisfies public traceable if the following conditions are satisfied: for all M_1, M_2, issue , for $(\text{pk}, \text{sk}) \leftarrow \mathbf{KeyGen}(1^\lambda), \sigma_1 \leftarrow \mathbf{Sign}(\text{sk}_i, T, M_1)$, and $\sigma_2 \leftarrow \mathbf{Sign}(\text{sk}_j, T, M_2)$, it holds with an overwhelming probability of equation (1).

2.4.2. Security Definitions. We use the security model in [5]. The security requirements of traceable ring signatures include the following three properties: tag-linkability, anonymity, and exculpability. The requirement of unforgeability (as defined in ordinary ring signatures) is not essential because the signature is unforgeable if a TRS satisfies both tag-linkability and exculpability [5].

Suppose \mathcal{A} is a probabilistic polynomial time (PPT) adversary and the security parameter is λ . Let N be the number of members in the ring; $T = (\overline{pk}, \text{issue})$ be the tag. By $\text{negl}(n, R)$, we denote a function which is negligible on the parameters n and R .

(1) *Tag-Linkability.* Take the security parameter λ as input, output T , and $N + 1$ valid pairs of message/signature. The adversary can get N pairs of message/signature by accessing N pairs of public and secret keys. The adversary's advantage over the scheme is $\text{Adv}_{\mathcal{A}}^{\text{tagLink}}$:

$$\text{Adv}_{\mathcal{A}}^{\text{tagLink}}(\lambda, N) := \Pr[\text{Expt}^{\mathcal{A}}], \quad (4)$$

where $\text{Expt}^{\mathcal{A}}$ is

- (1) $(T, (M_1, \sigma_1), \dots, (M_N, \sigma_N)) \leftarrow \mathcal{A}(1^\lambda)$
- (2) If all $i \in 1, \dots, N+1$, $\mathbf{Ver}(T, M_i, \sigma_i) = 1$ and $i, j \in \{1, \dots, N+1\}, i \neq j$, $\mathbf{Trace}(T, M_i, M_j, \sigma_i, \sigma_j) = \text{accept}$.

If for all the PPT adversaries \mathcal{A} , $\text{Adv}_{\mathcal{A}}^{\text{tagLink}}(\lambda, N) \leq \text{negl}(\lambda, N)$, the scheme satisfies tag-linkability.

(2) *Anonymity.* Let \mathcal{A} be a PPT adversary, $(\text{pk}_0, \text{sk}_0)$, $(\text{pk}_1, \text{sk}_1)$ are two public/secret key pairs generated by $\mathbf{KeyGen}(1^\lambda)$. Consider the following game:

- (1) $(\text{pk}_i, \text{sk}_i) \leftarrow \mathbf{KeyGen}(1^\lambda), i \in \{0, 1\}$
- (2) $b \xleftarrow{\$}$
- (3) $b' \leftarrow_{\mathcal{A}} \mathbf{Sign}(\text{sk}_0, \cdot), \mathbf{Sign}(\text{sk}_1, \cdot), \mathbf{Sign}(\text{sk}_{b'}, \cdot) (\text{pk}_0, \text{pk}_1)$
- (4) If $b = b'$, output 1; otherwise, output 0.

Let $\mathbf{Sign}(\text{sk}_b, \cdot)$ be a signing oracle. \mathcal{A} cannot ask queries to $\mathbf{Sign}(\text{sk}_b, \cdot)$ with different tags nor can \mathcal{A} ask queries with the same tag to both $\mathbf{Sign}(\text{sk}_b, \cdot)$ and $\mathbf{Sign}(\text{sk}_0, \cdot)$ or $\mathbf{Sign}(\text{sk}_b, \cdot)$ and $\mathbf{Sign}(\text{sk}_1, \cdot)$. If the output of this game is 1, the adversary wins the game. The advantage that \mathcal{A} wins the game is

$$\text{Adv}_{\mathcal{A}}^{\text{anon}}(\lambda, N) := \Pr[b = b'] - \frac{1}{2}. \quad (5)$$

If $\text{Adv}_{\mathcal{A}}^{\text{anon}}(\lambda, N) \leq \text{negl}(\lambda, N)$, the scheme is anonymous.

(3) *Exculpability.* This requirement is presented to ensure the adversary \mathcal{A} cannot construct two valid pairs of message/signature without knowing the secret key sk_i of the user \mathcal{P}_i . The game is described as follows:

- (1) $(\text{pk}, \text{sk}) \leftarrow \mathbf{KeyGen}(1^\lambda)$
- (2) $(T, M_1, \sigma_1), (T, M_2, \sigma_2) \leftarrow_{\mathcal{A}} \mathbf{Sign}(\text{sk}, \cdot) (\text{pk})$
- (3) $a \leftarrow \mathbf{Trace}(T, M_1, \sigma_1, M_2, \sigma_2)$
- (4) output a .

In this game, $\mathbf{Ver}(T, M_1, \sigma_1) = 1$ and $\mathbf{Ver}(T, M_2, \sigma_2) = 1$. For the message/signature pairs that \mathcal{A} accesses the signing oracle $\mathbf{Sign}(\text{sk}, \cdot)$ cannot link to at least one of the σ_1 or σ_2 . This means that there is at least one message in M_1 and M_2 that has not been queried in the $\mathbf{Sign}(\text{sk}, \cdot)$. The advantage that \mathcal{A} wins the following game is

$$\text{Adv}_{\mathcal{A}}^{\text{excul}}(\lambda, N) = \Pr[a = \text{pk}] \quad (6)$$

If $\text{Adv}_{\mathcal{A}}^{\text{excul}}(\lambda, N) \leq \text{negl}(\lambda, N)$, the TRS satisfies exculpability.

3. A Code-Based TRS Scheme

3.1. *A Proof of Knowledge Protocol.* We use a so-called GStern's protocol in [10] to construct our TRS scheme. Given \mathbf{H}, \mathbf{G} and \mathbf{s}, \mathbf{r} in the GSD problem, the prover \mathcal{P}_i wants the verifier \mathcal{V} to confirm that he has a small weight vector \mathbf{e}

such that $\mathbf{H}\mathbf{e}^T = \mathbf{s}^T$ and $\mathbf{G}\mathbf{e}^T = \mathbf{r}^T$. In other words, the protocol is a proof of knowledge protocol for the GSD problem. To be self-contained, we give the detailed description in **Algorithm 1**, in which h denotes a cryptographic hash function.

The GStern's protocol satisfies the following three natures: completeness, special soundness, and honest-verifier zero-knowledge (HVZK) [10]. To construct our TRS scheme, we apply the code-based Merkle-tree accumulator [29] to GStern's protocol. The statistical zero-knowledge argument of the accumulator allows the prover \mathcal{P}_i to convince the verifier \mathcal{V} , under zero-knowledge conditions, that \mathcal{P} knows a value correctly accumulated into the code-based Merkle-tree root described above. Let the uniformly random matrix $\mathbf{B} \in \mathbb{Z}_2^{n \times m}$ and the accumulated value \mathbf{u} be the input. The goal of \mathcal{P}_i is to convince \mathcal{V} that he has a value \mathbf{d} and a valid witness w . The relationship with the accumulator is $R_{\text{acc}} = \{((\mathbf{B}, \mathbf{u}) \in \mathbb{Z}_2^{n \times m} \times \{0, 1\}^n, d \in \{0, 1\}^n, w \in \{0, 1\}^l \times (\{0, 1\}^m)^l) : \text{Verify}_{\mathbf{B}}(\mathbf{u}, \mathbf{d}, w)\} = 1\}$. The authors of [29] gave specific techniques how to reduce the relationship R_{acc} to the abstract relationship $R_{\text{abstract}} = \{(\mathbf{M}, \mathbf{v}), \mathbf{w} \in \mathbb{Z}_2^{K \times L} \times \mathbb{Z}_2^K \times \text{VALID} : \mathbf{M} \cdot \mathbf{w} = \mathbf{v}\}$, where $\mathbf{M}, \mathbf{w}, \mathbf{v}$ are obtained by doing some transforms to $\mathbf{B}, \mathbf{u}, \mathbf{d}$. In other words, if we want to construct relation R_{acc} , we only need to construct relation R_{abstract} . We summarize the above method into the new protocol Acc-GStern's protocol described in **Algorithm 2**. The COM denotes a commitment scheme and \mathcal{S} is a finite set, where each $\phi \in \mathcal{S}$ is associated with a permutation Γ_ϕ of L elements. In addition, VALID is a subset of $\{0, 1\}^L$.

Lemma 4. *The protocol presented in **Algorithm 2** is complete, special sound, and HVZK.*

Proof. Our new protocol is a combination of GStern's protocol and the accumulator protocol. If an honest prover follows the protocol, then he always gets accepted by the verifier. Thus, the protocol has perfect completeness. If there is a simulator who extracts a valid witness from two valid transcripts $(\text{com}, \text{ch}, \text{resp})$ and $(\text{com}, \text{ch}', \text{resp}')$ of Acc-GStern's protocol with $\text{ch} \neq \text{ch}'$, where $\text{com}, \text{ch}(\text{ch}')$ and $\text{resp}(\text{resp}')$ are commitments, challenges, and responses, respectively, he can extract a valid witness. We consider the following cases:

- (1) When $\text{ch} = 0$ and $\text{ch}' = 1$, the simulator can extract \mathbf{e} from \mathbf{y} and $\mathbf{y} + \mathbf{e}$. For $\phi_2 = \phi$, the simulator can extract \mathbf{w} from $\Gamma_\phi(\mathbf{w})$.
- (2) When $\text{ch} = 0$ and $\text{ch}' = 2$, the simulator can extract \mathbf{e} from δ and $\delta(\mathbf{e})$. For $\phi_3 = \phi$, the simulator can extract \mathbf{w} from $\Gamma_\phi(\mathbf{w})$ and ϕ .
- (3) When $\text{ch} = 1$ and $\text{ch}' = 2$, the simulator can extract \mathbf{e} from δ and $\delta(\mathbf{e})$ and the simulator can extract \mathbf{w} from \mathbf{r}_w and $\mathbf{w} \oplus \mathbf{r}_w$.

Finally, we prove HVZK of the protocol. When $b = 0$, the simulator easily reveals $\mathbf{y}, \mathbf{y} + \mathbf{e}, \Gamma_\phi(\mathbf{w})$, and $\Gamma_\phi(\mathbf{r}_w)$. When $b = 1$, the simulator gets \mathbf{x} , where $\mathbf{H}\mathbf{x}^T = \mathbf{s}^T$ and reveals a vector \mathbf{y} , where $\mathbf{M} \cdot (\mathbf{y} \oplus \mathbf{r}_w) \oplus \mathbf{v} = \mathbf{M} \cdot \mathbf{r}_w$. When $b = 2$, the

- (1) **Parameters:** n, k, t
- (2) **Private information:** $\mathbf{e} \in \mathbb{Z}_2^n$ and $w(\mathbf{e}) = t$.
- (3) **Public information:** $\mathbf{H}, \mathbf{G}, \mathbf{s}, \mathbf{r}$, where $\mathbf{H}\mathbf{e}^T = \mathbf{s}^T$ and $\mathbf{G}\mathbf{e}^T = \mathbf{r}^T$.
- (4) **The prover \mathcal{P}_i :**
 - (i) chooses $y^s \leftarrow$ and a permutation δ .
 - (ii) sets $\mathbf{c}_1 = h(\delta, \mathbf{H}\mathbf{y}^T, \mathbf{G}\mathbf{y}^T)$, $\mathbf{c}_2 = h(\delta(\mathbf{y}))$,
 - (iii) and $\mathbf{c}_3 = h(\delta(\mathbf{y} + \mathbf{e}))$.
 - (iv) sends $\mathbf{c}_1, \mathbf{c}_2$, and \mathbf{c}_3 .
- (5) **The verifier \mathcal{V} :** - sends $b^s \leftarrow$.
- (6) **The prover \mathcal{P}_i :**
 - (i) if $b = 0$, sets $f := \{\mathbf{y}, \delta\}$.
 - (ii) if $b = 1$, sets $f := \{\mathbf{y} + \mathbf{e}, \delta\}$.
 - (iii) if $b = 2$, sets $f := \{\delta(\mathbf{y}), \delta(\mathbf{e})\}$.
 - (iv) sends f .
- (7) **The verifier \mathcal{V} :**
 - (i) if $b = 0$, accepts if $h(\delta, \mathbf{H}\mathbf{y}^T, \mathbf{G}\mathbf{y}^T) = \mathbf{c}_1$ and $h(\delta(\mathbf{y})) = \mathbf{c}_2$.
 - (ii) if $b = 1$, accepts if $h(\delta, \mathbf{H}(\mathbf{y} + \mathbf{e})^T + \mathbf{s}^T, \mathbf{G}(\mathbf{y} + \mathbf{e})^T + \mathbf{r}^T) = \mathbf{c}_1$ and $h(\delta(\mathbf{y} + \mathbf{e})) = \mathbf{c}_3$.
 - (iv) if $b = 2$, accepts if $h(\delta(\mathbf{y})) = \mathbf{c}_2$, $h(\delta(\mathbf{y}) + \delta(\mathbf{e})) = \mathbf{c}_3$, and $w(\delta(\mathbf{e})) = t$.

ALGORITHM 1: GStern's protocol.

- (1) **Parameters:** $n, k, t, K, L \in \mathbb{N}, L \geq K$.
- (2) **Private information:** \mathbf{e}, \mathbf{w} .
- (3) **Public information:**
 - (i) $\mathbf{H}, \mathbf{s}, \mathbf{G}, \mathbf{r}$, where $\mathbf{H}\mathbf{e}^T = \mathbf{s}^T$ and $\mathbf{G}\mathbf{e}^T = \mathbf{r}^T$.
 - (ii) \mathbf{M}, \mathbf{v} , where $\mathbf{M} \cdot \mathbf{w} = \mathbf{v}$.
- (4) **The prover \mathcal{P} :** - chooses $\mathbf{y}^s \leftarrow$, $\mathbf{r}_w^s \leftarrow$, a permutation δ , a permutation $\phi^s \leftarrow$, randomness ρ_1, ρ_2, ρ_3 for COM .
 - (i) sets $\mathbf{c}_1 = h(\delta, \mathbf{H}\mathbf{y}^T, \mathbf{G}\mathbf{y}^T)$, $\mathbf{c}_2 = h(\delta(\mathbf{y}))$, and $\mathbf{c}_3 = h(\delta(\mathbf{y} + \mathbf{e}))$.
 - (ii) sets $C_1 = COM(\phi, \mathbf{M} \cdot \mathbf{r}_w; \rho_1)$, $C_2 = COM(\Gamma_\phi(\mathbf{r}_w); \rho_2)$. and $C_3 = COM(\Gamma_\phi(\mathbf{w} \oplus \mathbf{r}_w); \rho_3)$.
- (iii) sends $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, C_1, C_2$, and C_3 .
- (5) **The verifier \mathcal{V} :**
 - (i) sends $b \leftarrow$.
- (6) **The prover \mathcal{P} :**
 - (i) if $b = 0$, computes $\mathbf{t}_w = \Gamma_\phi(\mathbf{w})$, $\mathbf{t}_r = \Gamma_\phi(\mathbf{r}_w)$, sets $f := \{\mathbf{y}, \delta, \mathbf{t}_w, \mathbf{t}_r, \rho_2, \rho_3\}$.
 - (ii) if $b = 1$, computes $\mathbf{w}_2 = \mathbf{w} \oplus \mathbf{r}_w$, $\phi_2 = \phi$, sets $f := \{\mathbf{y} + \mathbf{e}, \delta, \phi_2, \mathbf{w}_2, \rho_1, \rho_3\}$.
 - (iii) if $b = 2$, computes $\phi_3 = \phi$, $\mathbf{w}_3 = \mathbf{r}_w$, sets $f := \{\delta(\mathbf{y}), \delta(\mathbf{e}), \phi_3, \mathbf{w}_3, \rho_1, \rho_2\}$.
 - (iv) sends f .
- (7) **The verifier \mathcal{V} :**
 - (i) if $b = 0$, accepts if $h(\delta, \mathbf{H}\mathbf{y}^T, \mathbf{G}\mathbf{y}^T) = \mathbf{c}_1, h(\delta(\mathbf{y})) = \mathbf{c}_2, \mathbf{t}_w \in \text{VALID}, C_2 = COM(\mathbf{t}_r; \rho_2), C_3 = COM(\mathbf{t}_w \oplus \mathbf{t}_r; \rho_3)$.
 - (ii) if $b = 1$, accepts if $h(\delta, \mathbf{H}(\mathbf{y} + \mathbf{e})^T + \mathbf{s}^T, \mathbf{G}(\mathbf{y} + \mathbf{e})^T + \mathbf{r}^T) = \mathbf{c}_1, h(\delta(\mathbf{y} + \mathbf{e})) = \mathbf{c}_3, C_1 = COM(\phi_2, \mathbf{M} \cdot \mathbf{w}_2 \oplus \mathbf{v}; \rho_1)$ and $C_3 = COM(\Gamma_\phi(\mathbf{w}_2); \rho_3)$.
 - (iii) if $b = 2$, accepts if $h(\delta(\mathbf{y})) = \mathbf{c}_2, h(\delta(\mathbf{y}) + \delta(\mathbf{e})) = \mathbf{c}_3, w(\delta(\mathbf{e})) = t, C_1 = COM(\phi_3, \mathbf{M} \cdot \mathbf{w}_3; \rho_1)$ and $C_2 = COM(\Gamma_\phi(\mathbf{w}_3); \rho_2)$.

ALGORITHM 2: Acc-GStern's protocol.

simulator obtains a vector with weight t and a vector of length L . \square

3.2. Description of the Scheme. In this section, we give the description of our new TRS scheme in **Algorithm 3**. Generally speaking, the scheme is constructed by using the noninteractive protocol $\prod := (\text{Setup}, \mathcal{P}, \mathcal{V})$ which is obtained by combining Acc-GStern's protocol with Fiat-Shamir transform [30].

First, we use the public information T and a collision-resistant hash function h_1 to construct the matrix \tilde{H} . Then,

we construct a set of random syndromes $\mathbf{r}_1, \mathbf{r}_2, \dots, \mathbf{r}_L$, one of which, i.e., some \mathbf{r}_i , is a vector associated with the secret key of the actual signer. When the same signer signs two different messages with the same tag, the vector \mathbf{r}_i will be the same and so we can identify the signer. We also use a collision-resistant hash function g to generate the other \mathbf{r}_j , where $j \neq i$, to prevent the signer from cheating.

Let $\mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_L$ be the members of the ring, and $\overline{pk} = (pk_1, pk_2, \dots, pk_L)$ be the public keys of the members. The tag is $T = (\text{issue}, \overline{pk})$. Let issue be a string of signed targets (for example, an election or a transaction). Let $h_1: \mathbb{Z}_2^* \rightarrow \mathbb{Z}_2^{(n-k) \times n}$, $g: \mathbb{Z}_2^* \rightarrow \mathbb{Z}_n^{(n-k)}$ and h_2 be three

- (1) **Parameters:** $n, t, c, r, k' \in \mathbb{N}$, $m = 2 \cdot 2^c \cdot k' / c$, $k = 3n/4$, $\mathbf{H} \leftarrow \mathbb{S}$.
- (2) **KeyGen:** For each user \mathcal{P}_i , $i \in [L]$
- (i) randomly chooses $\mathbf{e}_i \in \{0, 1\}^n$ such that $w(\mathbf{e}_i) = t$.
 - (ii) computes $\mathbf{s}_i^T = \mathbf{H}\mathbf{e}_i^T$.
 - (iii) the private key: \mathbf{e}_i .
 - (iv) the public key: $\mathbf{H}, \mathbf{B}, \mathbf{s}_i$.
- (3) **Sign:** To generate a signature on message (HTML translation failed), the user \mathcal{P}_i
- (i) computes $\tilde{H} = h_1(T)$ and $\tilde{H}\mathbf{e}_i^T = \mathbf{r}_i^T$.
 - (ii) sets $A_0 = \mathbf{r}_i + g(M) + \dots + g^i(M)$.
 - (iii) computes $\mathbf{r}_j = A_0 + g(M) + \dots + g^j(M)$, for $j \in [L]$, $j \neq i$.
 - (iv) computes $\mathbf{d}_i = h_2(\mathbf{s}_i, \mathbf{r}_i)$, for all $i \in [L]$, and defines $R = (\mathbf{d}_i)_{i \in [L]}$.
 - (v) computes $\mathbf{u} = \text{Accu}_{\mathbb{B}}(R)$ and $\mathbf{w}_i = \text{WitGen}_{\mathbb{B}}(R, \mathbf{d}_i)$.
 - (vi) let $X := (\mathbf{H}, \tilde{H}, \mathbf{s}_i, \mathbf{B}, \mathbf{d}_i, \mathbf{u})$ be the public input of the protocol Π , and let $W := (\mathbf{w}_i, \mathbf{e}_i)$ be the secret inputs. Then, the user runs \mathcal{P} to generate a noninteractive proof ν .
 - (vii) outputs the signature $\sigma = (\nu, A_0)$.
- (4) **Verify:** To verify the signature σ on message M , the verifier
- (i) computes $\mathbf{r}_i = A_0 + g(M) + g^2(M) \dots + g^i(M)$, for all $i \in [L]$.
 - (ii) computes $\mathbf{d}_i = h_2(\mathbf{s}_i, \mathbf{r}_i)$, for all $i \in [L]$, and defines $R = (\mathbf{d}_i)_{i \in [L]}$.
 - (iii) computes $\mathbf{u} = \text{Accu}_{\mathbb{B}}(R)$.
 - (iv) let $X := (\mathbf{H}, \tilde{H}, \mathbf{s}_i, \mathbf{r}_i, \mathbf{B}, \mathbf{d}_i, \mathbf{u})$ be the public input of the protocol Π . Then, the verifier runs \mathcal{V} to get μ .
 - (v) if $\mu = 1$, outputs 1. Otherwise, outputs 0.
- (5) **Trace:** When the verifier is given two signatures (T, M, σ) and (T, M', σ') , where $\sigma = (\nu, A_0)$ and $\sigma' = (\nu', A'_0)$, the verifier
- (i) if $\text{Verify}(T, M, \sigma) = 1$ and $\text{Verify}(T, M', \sigma') = 1$, continue.
 - (ii) computes $\mathbf{r}_j = A_0 + g(M) + \dots + g^j(M)$ and $\mathbf{r}'_j = A'_0 + g(M') + \dots + g^j(M')$ for all $j \in [L]$.
 - (iii) if $\mathbf{r}_j = \mathbf{r}'_j$ for all $j \in [L]$, outputs linked.
 - (iv) else if only one index $j \in [L]$ makes $\mathbf{r}_j = \mathbf{r}'_j$, outputs pk_j .
 - (v) otherwise, outputs accept.

ALGORITHM 3: Our TRS scheme.

different collision-resistant hash functions. The hash function h_2 is the special function used in the accumulator as we defined in Definition 4. In addition, $g^i(x)$ is the function g applied i times on input x .

4. Security and Analysis

In this section, we present the analysis of our TRS scheme from two aspects: correctness analysis and security analysis.

4.1. Correctness Analysis. If a TRS scheme satisfies completeness and public traceability which are given in Definition 5 and Definition 6, respectively, we say that the TRS scheme is correct.

4.1.1. Completeness. The completeness of our TRS is easily verified. Since h and g are collision-resistant hash functions, and A_0 is generated by the tag and the secret key \mathbf{e}_i , the signer can always generate all \mathbf{r}_i and \mathbf{d}_i for all $i \in [L]$, just like in the signing algorithm. The verifier can recover all \mathbf{r}_i from A_0 and also recover all \mathbf{d}_i . Due to the completeness of the underlying protocol, the output of the verification algorithm is always 1 when the input of the verification algorithm is the honest signature ν .

4.1.2. Public Traceability. Next, we give the proof of public traceability from three cases:

- (i) Case 1. Suppose that $M = M'$, $i = i'$. Therefore, we have $\mathbf{r}_i^T = h_1(T)\mathbf{e}_i^T = h_1(T)\mathbf{e}_i^T = \mathbf{r}_i^T$, and we get $\mathbf{r}_j = \mathbf{r}'_j$ for all $j \in [L]$. In this case, the output of **Trace** is always linked.
- (ii) Case 2. Suppose that $M \neq M'$, $i = i'$. So, we have $\mathbf{r}_i^T = h_1(T)\mathbf{e}_i^T = h_1(T)\mathbf{e}_i^T = \mathbf{r}_i^T$. However, due to the collision resistance of the hash function g , we have $\mathbf{r}_j \neq \mathbf{r}'_j$, for $j \in [L]$, $j \neq i$ with overwhelming probability. Therefore, only $\mathbf{r}_i = \mathbf{r}'_i$ in the two sequences $(\mathbf{r}_j)_{j \in [L]}$ and $(\mathbf{r}'_j)_{j \in [L]}$. In this case, the output of **Trace** is always pk_i .
- (iii) Case 3. Suppose that $i \neq i'$ and $M = M'$. Thus, we have $\mathbf{r}_i^T = h_1(T)\mathbf{e}_i^T$, $h_1(T)\mathbf{e}_{i'}^T = \mathbf{r}_{i'}^T$, and $\mathbf{r}_i \neq \mathbf{r}_{i'}$. Then, due to the hash function, we have $\mathbf{r}_j \neq \mathbf{r}'_j$ for all $j \in [L]$ with overwhelming probability. If $i \neq i'$ and $M \neq M'$, we obtain $\mathbf{r}_i \neq \mathbf{r}'_i$. If the output of the algorithm **Trace** is not *accept*, there must be some $j \neq i$, $j \in [L]$, satisfying $\mathbf{r}_j = \mathbf{r}'_j$. However, we have $\mathbf{r}_j = A_0 + g(M) + \dots + g^j(M)$ and $\mathbf{r}'_j = A'_0 + g(M') + \dots + g^j(M')$. Due to the collision resistance of hash functions and the difficulty of the GSD problem, the probability of the existence of \mathbf{r}_j and \mathbf{r}'_j is negligible. Therefore, the output of **Trace** is *accept* with overwhelming probability.

4.2. Security Analysis. We use the security definition of TRS in [5], which formalized security requirements called anonymity, tag-linkability, and exculpability.

Theorem 1. *Our scheme is secure in the random oracle model, i.e., satisfying anonymity, tag-linkability, and exculpability.*

We prove Theorem 1 from the following three aspects: proof for anonymity, proof for tag-linkability, and proof for exculpability.

4.2.1. Proof for Anonymity. To show that our scheme satisfies anonymity, we define a PPT adversary \mathcal{A} , a challenger \mathcal{C} , and a series of games G_i , $i = 0, 1, 2, 3, 4$. There are three signing oracles: \mathbf{Sign}_{sk_0} , \mathbf{Sign}_{sk_1} , \mathbf{Sign}_b . The advantage of the adversary \mathcal{A} in G_i is denoted by $\text{Adv}_{\mathcal{A}, G_i}^{\text{anon}}$.

G_0 : this game is just like the game defined in (2), in which $b = 0$. The adversary \mathcal{A} can access three oracles. The challenger \mathcal{C} honestly runs the \mathbf{Sign}_{sk_i} oracle with corresponding secret keys to reply to \mathcal{A} 's queries to these three oracles.

G_1 : let (S_p, S_o) be the simulators of the protocol Π . The challenger \mathcal{C} runs S_o to simulate the public parameters, instead of running **Setup** of the protocol Π . When the adversary \mathcal{A} makes queries to \mathbf{Sign}_{sk_b} , the challenger \mathcal{C} runs S_p to answer the query.

Due to Definition 3, we have

$$\text{Adv}_{\mathcal{A}, G_0}^{\text{anon}}(\lambda) \approx \text{Adv}_{\mathcal{A}, G_1}^{\text{anon}}(\lambda). \quad (7)$$

G_2 : the difference between G_2 and G_1 is that the challenger \mathcal{C} creates an empty table δ . We assume that the sequence $(\mathbf{r}_1^{(i)}, \mathbf{r}_2^{(i)}, \dots, \mathbf{r}_L^{(i)})$ is computed by the user \mathcal{P}_i , and i is the position of pk_i in T . The adversary \mathcal{A} gets access to \mathbf{Sign}_{sk_b} and the query is (T, M) . The challenger \mathcal{C} does not use $h_1(T)\mathbf{e}_b^T$ to get $\mathbf{r}_b^{(b)}$. The challenger \mathcal{C} checks whether there is a tuple $(T, M, \mathbf{r}_*^{(b)})$ in δ , where $\mathbf{r}_*^{(b)}$ is the vector in δ together with (T, M) . If the tuple exists, then \mathcal{C} uses $\mathbf{r}_*^{(b)}$ and runs the simulator S_p to generate the signature. Otherwise, the challenger \mathcal{C} randomly chooses a vector $\mathbf{r}_*^{(b)} \xleftarrow{\$}$, sets $\mathbf{r}_*^{(b)} = \mathbf{r}_b^{(b)}$, and adds $(T, M, \mathbf{r}_*^{(b)})$ to δ . Then, the challenger \mathcal{C} generates the signature using $\mathbf{r}_*^{(b)}$.

Due to the GSD problem, the adversary cannot calculate \mathbf{e} from $\mathbf{r}_b^{(b)}$ and the public parameters. So, \mathcal{A} cannot distinguish G_1 and G_2 :

$$\text{Adv}_{\mathcal{A}, G_1}^{\text{anon}}(\lambda) \approx \text{Adv}_{\mathcal{A}, G_2}^{\text{anon}}(\lambda). \quad (8)$$

G_3 : the difference between G_3 and G_2 is that the challenger \mathcal{C} uses \mathbf{sk}_1 to generate \mathbf{r}_j and answers the query to \mathbf{Sign}_{sk_b} . G_4 : the difference between G_0 and G_4 is the value of b . G_4 defines $b = 1$.

Due to the zero-knowledge property of the underlying protocol and the hardness of the GSD problem, the outputs of all the above games contain nothing about b . Therefore, the adversary can guess the right b with probability $1/2$ and the advantage that the adversary \mathcal{A} wins the game is negligible.

4.2.2. Proof for Tag-Linkability. We assume that the PPT adversary is \mathcal{A} and the sequence $(\mathbf{r}_i)_{i \in [L]}$ is contained in the signature which can be reconstructed from (T, M_i, ν_i, A_0) . The $(L+1)$ message/signature pairs $(M_1, \sigma_1), \dots,$

(M_{L+1}, σ_{L+1}) with tag T are generated by the adversary \mathcal{A} . Suppose that \mathcal{A} wins the tag-linkability game. Thus, we have (a) $\mathbf{Verify}(\sigma_i, M_i, T) = 1, \forall i \in [L+1]$; and (b) $\mathbf{Trace}(T, M_i, \sigma_i, M_j, \sigma_j) = \text{accept}, \forall i, j \in [L+1], i \neq j$.

Let I_{real} and I_{S_o} be the sets of all the parameters honestly generated in our construction and all the parameters generated by the simulator S_o , respectively. Due to the zero-knowledge property of the protocol, \mathcal{A} cannot distinguish I_{real} and I_{S_o} . Therefore, there is an extractor that can extract a witness $w = (i, \mathbf{e}_i)$ for each (M_i, σ_i) . There is at most only one witness with overwhelming probability because of the hardness of the GSD problem, and correspondingly, $\mathbf{s}_i^T = \mathbf{He}_i^T$ and $\mathbf{r}_i^T = h_1(T)\mathbf{e}_i^T, i \in [L+1]$. Since T only contains L public keys, there must exist $\mathbf{s}_i = \mathbf{s}_j, i \neq j$ in the sequence $(\text{pk}_i)_{i \in [L+1]}$. Since all public keys in T are distinct, we have $\mathbf{e}_i = \mathbf{e}_j$. Finally, we get $\mathbf{r}_i^T = h_1(T)\mathbf{e}_i^T = h_1(T)\mathbf{e}_j^T = \mathbf{r}_j^T$, which means that two signatures σ_i and σ_j cannot be accepted by **Trace**. However, this contradicts our previous assumptions.

4.2.3. Proof for Exculpability. Suppose that \mathcal{A} is a PPT adversary. We define the following games $G_i, i = 0, 1$.

G_0 : this is the real exculpability game. In this game, the challenger \mathcal{C} runs **KeyGen** to generate $(\text{pk}_j, \text{sk}_j)$, where j is the position of pk_j in T . \mathcal{C} runs \mathbf{Sign}_{sk_j} to reply to \mathcal{A} 's queries to \mathbf{Sign}_{sk_j} .

G_1 : the challenger \mathcal{C} runs the simulator of the protocol Π to generate the public parameters and randomly chooses $\mathbf{s}_i \xleftarrow{\$}$. \mathcal{C} creates an empty table δ to record each query. The challenger \mathcal{C} receives a query (T, M) to \mathbf{Sign}_{sk_j} and the secret key sk_j corresponds to the public key pk_j in T , where (HTML translation failed) is the position of pk_j in T . However, \mathcal{C} does not compute $\mathbf{r}_j^{(j)}$ in terms of $h_1(T)\mathbf{e}_j^T$. If $(T, M, \mathbf{r}_*^{(j)})$ is not in the table δ , where $\mathbf{r}_*^{(j)}$ is the vector in δ together with (T, M) , he randomly chooses a vector $\mathbf{r}_*^{(j)} \xleftarrow{\$}$ and adds $(T, M, \mathbf{r}_*^{(j)})$ to the table δ and generates the signature with $\mathbf{r}_*^{(j)}$. Otherwise, \mathcal{C} sets $\mathbf{r}_j^{(j)}$ as $\mathbf{r}_*^{(j)}$ and uses the simulator S_p to generate the signature.

Due to the zero-knowledge property of the underlying protocol and the hardness of the GSD problem, the advantage that \mathcal{A} distinguishes G_0 and G_1 is

$$\text{Adv}_{\mathcal{A}, G_0}^{\text{excul}}(\lambda) \approx \text{Adv}_{\mathcal{A}, G_1}^{\text{excul}}(\lambda). \quad (9)$$

Then, we show that a successful attack is impossible in G_1 . If \mathcal{A} can output two valid pairs (T, M, σ) and (T, M', σ') , the two valid pairs can satisfy:

- (1) $\mathbf{Verify}(T, M, \sigma) = 1$ and $\mathbf{Verify}(T, M', \sigma') = 1$,
- (2) $\mathbf{Trace}(T, M, \sigma, M', \sigma') = \text{pk}_i$, where i is the position of pk_i in T .

We consider the following two cases:

- (i) Case 1. Suppose that one of those two pairs can be linked with the table δ and the pair is $(T, M', \sigma' = (\nu', A_0'))$. Therefore, there is a pair $(T, M^*, \sigma^* = (\nu^*, A_0))$ in δ that can be linked with $(T, M', \sigma' = (\nu', A_0'))$ where M^* and σ^* are the

TABLE 1: Our TRS scheme.

Scheme	n	k	t	c	k'	r	L	p	Pk size (bit)	Signature size (bit)	Security
1	2400	2006	58	8	896	509	3	220	3.0×10^7	7.9×10^7	128
2	4150	3307	132	14	1792	1024	3	440	4.2×10^9	1.1×10^{10}	256

vectors in δ in the target pair and (v^*, A_0) are the vectors corresponding to σ^* . We can get a witness $w = (i', \mathbf{e}_i')$ from the extractor of the protocol Π . In this way, the elements in the pair should satisfy $\mathbf{s}_i'^T = H\mathbf{e}_i'^T$, $\mathbf{r}_i'^T = h_1(T)\mathbf{e}_i'^T$ and $\mathbf{r}_j' = A_0 + g(M') + \dots + g^j(M')$ for all $j \in [L]$, $j \neq i$, and due to that the two pairs are linked, $\mathbf{s}^* = \mathbf{s}_i'$ and $\mathbf{r}_j^* = \mathbf{r}_j'$, for all $j \in [L]$. However, \mathbf{s}^* is generated by the simulator of the protocol Π and the vectors \mathbf{r}_j^* , $j \in [L]$ are randomly chosen in \mathbb{Z}_2^{n-k} in G_1 . Considering the hardness of the GSD problem, the adversary \mathcal{A} cannot generate the valid \mathbf{e}' and \mathbf{r}' .

- (ii) Case 2. Suppose that neither of the two pairs can be associated with the table δ . So, we have $\mathbf{r}_j = \mathbf{r}_j'$, which means that $A_0 + g(M) + \dots + g^j(M) = A_0 + g(M') + \dots + g^j(M')$, for all $j \in [L]$. We can also extract the witness (i, \mathbf{e}_i) and (i', \mathbf{e}_i') from v and v' , respectively. We have $h_1(T)\mathbf{e}_i^T = \mathbf{r}_i^T$ and $h_1(T)\mathbf{e}_i'^T = \mathbf{r}_i'^T$, which holds that $h_1(T)\mathbf{e}_i^T = h_1(T)\mathbf{e}_i'^T$. If $i = i'$, the **Trace** will output \mathbf{s}_i . However, \mathbf{r}_i is chosen randomly in \mathbb{Z}_2^{n-k} in G_1 , and so \mathcal{A} cannot construct a vector \mathbf{e}_i which satisfies $H\mathbf{e}_i^T = \mathbf{s}_i^T$ and $h_1(T)\mathbf{e}_i^T = \mathbf{r}_i^T$. In this condition, we have $i \neq i'$. Due to the hardness of the GSD problem, the probability that the adversary \mathcal{A} constructs the valid $\mathbf{e}_i, \mathbf{e}_i', \mathbf{r}_i, \mathbf{r}_i'$ is negligible. Therefore, the adversary \mathcal{A} cannot have a successful attack.

5. Efficiency

In this section, we consider the efficiency of our scheme in three aspects: public key sizes, secret key sizes, and signature sizes.

- (1) **Public key size:** the public key in our scheme consists of $(\mathbf{H}, \mathbf{B}) \in \mathbb{Z}_2^{(n-k) \times n} \times \mathbb{Z}_2^{r \times m}$ and vectors $\mathbf{s}_i \in \mathbb{Z}_2^{n-k}$, for $i \in [L]$. The public key size of our scheme is $n^2 - k(n+L) + rm + Ln$ bits.
- (2) **Secret key size:** the secret key of each signer \mathcal{P}_i is a vector $\mathbf{e}_i \in \mathbb{Z}_2^n$, and the bit length of \mathbf{e}_i is n .
- (3) **Signature size:** the signature size in our scheme is determined by the proof v , and the bit length of the signature is $O(\lambda \cdot \log L)$. Specifically, the signature size of our scheme includes the following three aspects: (i) the size of three hash values and three commitments is 6λ bits, where λ is the security parameter. (ii) For each case, $b = 0$, $b = 1$, or $b = 2$, the size of response is $4lm + 4nl - 2n + 2\lambda$ bits, where $l = \log L$. (iii) The bit size of the vector A_0 is $n - k$. The repetition number of Acc-GStern's protocol is defined as p (for example, if the cheating probability of Acc-GStern's protocol is approximately 2^{-128} , $p = 220$). To sum up, the signature size

of our scheme is $6\lambda + 4lm + 4nl - 2n + 2p\lambda + n - k$ bits. Since $l = \log L$ and L is the ring size, our signature size is logarithmic in the ring size.

According to decoding attacks in [34–36], we set the parameters of our scheme under 128 bit and 256 bit security in Table 1.

We give the implementation of our scheme on an Intel(R) Core(TM) i5-1035G1 CPU @ 2.20 GHz, and we implemented our scheme based on Python. We use the first set of parameters in Table 1 to implement our scheme. The running time of **KeyGen** to generate a pair of (pk, sk) is about 3 ms. However, due to the use of the hash function defined in Definition 4, the total running time for our signature scheme to generate a signature is about 2 minutes.

Since our scheme is an improvement over [10], the signature size in the original scheme is linear in the number of ring size, while the signature size of our scheme is logarithmic in the ring size. To the best of our knowledge, there are no other code-based TRS schemes. However, for some applications, the key and signature sizes of our scheme are still large. Finding new techniques to reduce the sizes of code-based traceable ring signature schemes and improve the efficiency of code-based traceable ring signature schemes are our future research direction.

6. Conclusion

In this paper, we construct a new code-based TRS scheme. The signature size of our scheme is logarithmic in the size of the ring. We then provide the tag-linkability, anonymity, and exculpability of our scheme and so our scheme is secure in the random oracle model under the assumption of the hardness of the SD problem and the 2-RNSD problem.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The work of L.P. Wang was supported in part by the National Natural Science Foundation of China (Grant no. 61872355), Mathematical Tianyuan Foundation of National Natural Science Foundation of China (Grant No.12026427), and National Key Research and Development Program of China (No. 2018YFA0704703).

References

- [1] E. Fujisaki, "Sub-linear size traceable ring signatures without random oracles," in *Proceedings of the Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011*, pp. 393–415, Springer, San Francisco, CA, USA, 14 February 2011.
- [2] C. Hu and D. Li, "Forward-secure traceable ring signature," in *Proceedings of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, pp. 200–204, IEEE Computer Society, Qingdao, China, 30 July 2007.
- [3] X. Bultel and P. Lafourcade, "k-times full traceable ring signature," in *Proceedings of the 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*, pp. 39–48, IEEE, Salzburg, Austria, 31 August 2016.
- [4] S. S. M. Chow, J. K. Liu, and D. S. Wong, "Robust receipt-free election system with ballot secrecy and verifiability," in *Proceedings of the Network and Distributed System Security Symposium, NDSS 2008*, The Internet Society, San Diego, California, USA, 24 February 2008.
- [5] E. Fujisaki and K. Suzuki, "Traceable ring signature," in *Proceedings of the Public Key Cryptography - PKC 2007, 10th International Conference on Practice and Theory in Public-Key Cryptography*, pp. 181–200, Springer, Beijing, China, 16 April 2007.
- [6] M. H. Au, J. K. Liu, W. Susilo, and T. H. Yuen, "Secure id-based linkable and revocable-iff-linked ring signature with constant-size construction," *Theoretical Computer Science*, vol. 469, no. 1–14, pp. 1–14, 2013.
- [7] F. Tang, J. Pang, K. Cheng, and Q. Gong, "Multiauthority traceable ring signature scheme for smart grid based on blockchain," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 5566430, 9 pages, 2021.
- [8] X. Peng, K. Gu, Z. Liu, and W. Zhang, "Traceable identity-based ring signature for protecting mobile iot devices," in *Proceedings of the Data Mining and Big Data - 6th International Conference, DMBD 2021*, pp. 158–166, Springer, Guangzhou, China, 20 October 2021.
- [9] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, IEEE Computer Society, Santa Fe, New Mexico, USA, 20 November 1994.
- [10] P. Branco and P. Mateus, "A traceable ring signature scheme based on coding theory," in *Proceedings of the International Conference on Post-Quantum Cryptography*, pp. 387–403, Springer, Chongqing, China, 29 May 2019.
- [11] R. Cramer, I. Damgård, and B. Schoenmakers, "Proofs of partial knowledge and simplified design of witness hiding protocols," in *Proceedings of the Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference*, pp. 174–187, Springer, Santa Barbara, California, USA, 21 August 1994.
- [12] H. Feng, J. Liu, Q. Wu, and Y.-N. Li, "Traceable ring signatures with post-quantum security," in *Proceedings of the Topics in Cryptology - CT-RSA 2020 - The Cryptographers' Track at the RSA Conference 2020*, pp. 442–468, Springer, San Francisco, CA, USA, 24 February 2020.
- [13] A. Scafuro and B. Zhang, "One-time traceable ring signatures," in *Proceedings of the Computer Security - ESORICS 2021 - 26th European Symposium on Research in Computer Security*, pp. 481–500, Springer, Darmstadt, Germany, 4 October 2021.
- [14] H. Feng, J. Liu, D. Li, Y.-N. Li, and Q. Wu, "Traceable ring signatures: general framework and post-quantum security," *Designs, Codes and Cryptography*, vol. 89, no. 6, pp. 1111–1145, 2021.
- [15] N. T. Courtois, M. Finiasz, and N. Sendrier, "How to achieve a mcEliece-based digital signature scheme," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, pp. 157–174, Springer, 2001.
- [16] N. Aragon, O. Blazy, P. Gaborit, A. Hauteville, and G. Zémor, "Durandal: a rank metric based signature scheme," in *Proceedings of the Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 728–758, Springer, Darmstadt, Germany, 19 May 2019.
- [17] T. Debris-Alazard, N. Sendrier, and J.-P. Tillich, "Wave: a new family of trapdoor one-way preimage sampleable functions based on codes," in *Proceedings of the Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security*, pp. 21–51, Springer, Kobe, Japan, 8 December 2019.
- [18] E. Persichetti, "Efficient one-time signatures from quasi-cyclic codes: a full treatment," *Cryptography*, vol. 2, no. 4, p. 30, 2018.
- [19] D. Zheng, X. Li, and K. Chen, "Code-based ring signature scheme," *International Journal on Network Security*, vol. 5, no. 2, pp. 154–157, 2007.
- [20] P. Branco and P. Mateus, "A code-based linkable ring signature scheme," in *Proceedings of the Provable Security - 12th International Conference, ProvSec 2018*, pp. 203–219, Springer, Jeju, South Korea, 25 October 2018.
- [21] C. Aguilar Melchor, P.-L. Cayrel, P. Gaborit, and F. Laguillaumie, "A new efficient threshold ring signature scheme based on coding theory," *IEEE Transactions on Information Theory*, vol. 57, no. 7, pp. 4833–4842, 2011.
- [22] L. Dallot and D. Vergnaud, "Provably secure code-based threshold ring signatures," in *Proceedings of the Cryptography and Coding, 12th IMA International Conference, Cryptography and Coding 2009*, pp. 222–235, Springer, Cirencester, UK, 15 December 2009.
- [23] H. Assidi, E. B. Ayebie, and E. M. Souidi, "An efficient code-based threshold ring signature scheme," *Journal of Information Security and Applications*, vol. 45, pp. 52–60, 2019.
- [24] Q. Alamélou, O. Blazy, S. Cauchie, and P. Gaborit, "A practical group signature scheme based on rank metric," in *Proceedings of the Arithmetic of Finite Fields - 6th International Workshop, WAIFI 2016*, pp. 258–275, Springer, Ghent, Belgium, 13 July 2016.
- [25] M. F. Ezerman, H. T. Lee, S. Ling, K. Nguyen, and H. Wang, "A provably secure group signature scheme from code-based assumptions," in *Proceedings of the Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security*, pp. 260–285, Springer, Auckland, New Zealand, 29 December 2015.
- [26] B. E. Ayebie, H. Assidi, and E. M. Souidi, "A new dynamic code-based group signature scheme," in *Proceedings of the Codes, Cryptology and Information Security - Second International Conference, C2SI 2017*, pp. 346–364, Springer, Rabat, Morocco, 10 April 2017.
- [27] Q. Alamélou, O. Blazy, S. Cauchie, and P. Gaborit, "A code-based group signature scheme," *Designs, Codes and Cryptography*, vol. 82, no. 1–2, pp. 469–493, 2017.

- [28] M. F. Ezerman, H. T. Lee, S. Ling, K. Nguyen, and H. Wang, "Provably secure group signature schemes from code-based assumptions," *IEEE Transactions on Information Theory*, vol. 66, no. 9, pp. 5754–5773, 2020.
- [29] K. Nguyen, H. Tang, H. Wang, and N. Zeng, "New code-based privacy-preserving cryptographic constructions," *Lecture Notes in Computer Science*, in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, pp. 25–55, Springer, Kobe, Japan, 4 December 2019.
- [30] A. Fiat and A. Shamir, "How to prove yourself: practical solutions to identification and signature problems," in *Proceedings of the Advances in Cryptology - CRYPTO '86*, pp. 186–194, Springer, Santa Barbara, California, USA, 11 August 1986.
- [31] E. Berlekamp, R. McEliece, and H. Van Tilborg, "On the inherent intractability of certain coding problems (corresp.)," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 384–386, 1978.
- [32] D. Augot, M. Finiasz, and N. Sendrier, "A family of fast syndrome based cryptographic hash functions," in *Proceedings of the Progress in Cryptology - Mycrypt 2005, First International Conference on Cryptology*, pp. 64–83, Springer, Kuala Lumpur, Malaysia, 28 September 2005.
- [33] Y. Zhang, D. He, F. Zhang, X. Huang, and D. Li, "An efficient blind signature scheme based on SM2 signature algorithm," in *Proceedings of the Information Security and Cryptology - 16th International Conference, Inscrypt 2020*, pp. 368–384, Springer, Guangzhou, China, 11 December 2020.
- [34] R. C. Torres and N. Sendrier, "Analysis of information set decoding for a sub-linear error weight," in *Proceedings of the Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016*, pp. 144–161, Springer, Fukuoka, Japan, 24 February 2016.
- [35] A. Becker, A. Joux, A. May, and A. Meurer, "Decoding random binary linear codes in $2^{n/20}$: how $1 + 1 = 0$ improves information set decoding," in *Proceedings of the Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 520–536, Springer, Cambridge, UK, 15 April 2012.
- [36] D. J. Bernstein, T. Lange, C. Peters, and P. Schwabe, "Faster 2-regular information-set decoding," in *Proceedings of the Coding and Cryptology - Third International Workshop, IWCC 2011*, pp. 81–98, Springer, Qingdao, China, 30 May 2011.

Review Article

A Summary of Security Techniques-Based Blockchain in IoV

Chen Chen¹ and Shi Quan ²

¹*School of Information Science and Technology, Nantong University, Nantong, China*

²*School of Transportation and Civil Engineering, Nantong University, Nantong, China*

Correspondence should be addressed to Shi Quan; sq@ntu.edu.cn

Received 28 October 2021; Revised 16 January 2022; Accepted 9 February 2022; Published 8 March 2022

Academic Editor: Haowen Tan

Copyright © 2022 Chen Chen and Shi Quan. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the rapid development of the informatization and industrialization of the Internet of Vehicles (IoV), the number and application of connected vehicles are growing rapidly. The safety problem is related to the property and life of human beings, which has attracted extensive attention from academic and industrial circles. Based on the study of high-quality literature published in the past decade and other high-level research works, this paper first analyzes the forms of attack against the Internet of Vehicles from the two aspects of attack mode and target. Then, it summarizes the existing blockchain-based system framework of the Internet of Vehicles (BIOV) and then discusses the security solutions of blockchain-based vehicles from the aspects of authentication, privacy, trust management, access control, and so on, to support the distributed system architecture and solve the security challenges of the Internet of Vehicles. Finally, the technical difficulties and the direction of further research of BIOV are summarized.

1. Introduction

IoV has become the most promising and fastest-growing new network paradigm and has also brought many applications, such as emergency communication of traffic incidents, traffic congestion prediction, and new traffic service modes. So in IoV, the secure transmission of V2X [1] is crucial. Suppose a hacker invades a regular vehicle or interferes with vehicle communications through eavesdropping, jamming, or spoofing attacks. In that case, there is a potential for serious accidents that can damage the vehicle or endanger the lives of passengers. Therefore, the primary safety goal of the Internet of Vehicles is to disseminate critical event information (such as accident reports) in a timely, safe, and accurate manner to ensure safe driving [2]. Most models of IoV are on centralized patterns. But the main problem with centralized mechanisms is the single point of failure problem. Many researchers have proposed distributed model schemes, but due to the dynamic nature of IoV, it has other issues, such as distributed vital management, content distribution, message trust, and data privacy. We should need a security mechanism to ensure that entities

in IoV cannot manipulate, alter, or delete critical event messages in VANET. If critical event messages generated by vehicle entities are in a distributed database, all information will be transparent and shared. The security technology-based blockchain can achieve this. Blockchain is a decentralized peer-to-peer network, and nodes do not need to trust each other. It includes data encryption, timestamps, distributed consensus, smart contracts, and other technologies. With the maturity of blockchain technology, it has been deeply integrated with various industries [3, 4], solving the technical bottlenecks unique to multiple industries. The integration of blockchain technology and IoV is also one of the current research hotspots.

Why can blockchain integrate with IoV? First, one of the main characteristics of blockchain is decentralization. We can use this feature to realize the rapid authentication of safety information on the Internet of Vehicles and achieve the purpose of traceability management of traffic accidents. By improving the traceability and transparency of related vehicle information, we provide the event-specific basis for decision-making. Second, because the blockchain is a decentralized, peer-to-peer trust-based network, the data in

the blockchain is reliable, accurate, consistent, timely, and widely accessible. It is resistant to malicious attacks and has no single point of failure [5]. In addition, blockchain can protect the security and privacy of vehicle nodes by using a hash function and encryption technology. All transactions and transactions in the blockchain are timestamped and authenticated using private keys, which can prevent malicious or forged messages; anonymized vehicle identities or data can protect user privacy. Therefore, blockchain has been applied to the Internet of Vehicles as a security mechanism, and related research has attracted increasing attention. For example, 30 companies, including BMW, Ford, Renault, General Motors and IBM, Bosch, and Blockchain, have joined MOBI's Mobility Open Blockchain initiative [6]. The mission of MOBI is to accelerate the application of blockchain. Ali et al. [7] are working on a project blockchain-based system, including designing and implementing a complete vehicle tracking lifecycle, from manufacturing, customs, registration, on the road, and violations to buying and selling.

This paper classifies attacks of IoV in terms of attack targets and methods. It then investigates security technology that combines IoV and blockchain, which are also the focus of this paper. Firstly, the network model system to BIoV is studied. Then, it discusses the security technology of BIoV, proposes the security analysis methods and evaluation parameters, and compares the currently popular methods. Finally, the future challenges and research directions of security technology are summarized.

2. Attack Categories

As early as 2005, Chavez et al. [8] suggested that hackers may attack cars, and identity authentication and encryption should keep cars safe. This section focuses on attack categories and security requirements of the IoV. Firstly, attacks of IoV can be classified into traditional security attacks and exclusive attacks, according to the target and mode. Conventional security attacks include physical control attacks, network layer attacks, identity attacks, forged information attacks, and application attacks. Exclusive attacks are common and seriously impact the IoV but do not exist or be uncommon and have little impact on the traditional network. The VeReMi [9] (an attack data set with tagged attributes), for example, launches five types of positional attacks by forging GPS positions.

2.1. Physical Control Attacks. IVI (In-Vehicle Infotainment) is an intelligent multimedia device integrated with the car center console, with radio, GPS navigation, entertainment, voice assistant, Bluetooth, WiFi, and other functions. Because of its ancillary functions and high integration, it has become an essential target for attackers. Through IVI, the attacker tries to open the system engineering mode and use ADB (Android Debug Bridge) or USB to connect. After the connection is successful, obtain the system login name and password by brute force. After the login succeeds, they try to raise the rights. If the operation succeeds, an attacker can

access any file in the IVI system to steal private data or critical information. They start or stop the vehicle's regular service [10] by tampering with the system configuration to bypass vehicle safety restrictions. It is a severe threat to the safety of vehicle function and information.

2.2. Network Attacks. The IoV is built on top of the traditional network. For example, the network of IoV also has the functions of routing and forwarding, logical addressing, and congestion control. Therefore, IoV faces the same security problems as traditional networks, such as DOS (Denial of Service)/DDOS (Distributed Denial of Service) [11], Black-Hole Attacks, Replay Attacks, and Grey Hole Attacks. In addition, automobiles are also under wireless threats [12] by using cellular networks (4G/5G), WiFi, Bluetooth, and LTE-V2X.

In a cellular network, an attacker establishes a pseudobase station, hijacks and monitors t-box session and communication data through conventional methods such as DNS hijacking, and obtains sensitive data (such as user sensitive information and vehicle status information).

2.2.1. WiFi Communication. By cracking the WiFi authentication password, the attacker can connect to the In-Vehicle Networking and obtain the sensitive and private data of the vehicle without authorization. Hackers can also exploit known vulnerabilities in operating systems to launch infiltration attacks.

2.2.2. Bluetooth Communication. Attackers can hijack traffic between Bluetooth keys and vehicles and tamper with and replay malicious traffic. Not only does it result in vehicle theft, but also it threatens the functional safety of the vehicle. In general, cellular networks are the more secure of the three wireless technologies.

2.3. Identity Attacks. There are two main attack entities for identity attacks: vehicles and roadside unit (RSU). In IoV, malicious nodes are often disguised as RSU and attempt to trick users into obtaining their authentication information. The attackers then use their identity to access confidential information, even as an authentication against others. In addition, they can also impersonate the identity of other vehicles. For example, an attacker might mimic an emergency vehicle, which would give them a higher priority in the network and thus reduce congestion.

2.4. Fake Information Attacks. The spread of false information [13] also exists in IoV, and it will cause more severe harm. Like Sybil Attacks by Douceur [14], attackers can spread incorrect information about road congestion, effectively forcing other vehicles to divert. They can also lead to traffic jams or sending accident alerts. Because of its low computing cost, falsifying information becomes one of the common attacks. And the distributed feature of IoV will lead to more severe harm.

2.5. Application Attacks. Applications related to IoV can be classified by function into vehicle control, query, and services (which provide the procedures required by safe and unsafe applications). The most common examples are malware and spyware. A malicious node inserts malware into a legitimate, intelligent connected vehicle application. Users are installing malware at the same time they download and install the software. The purpose of malware is to collect vehicle terminal location information, authentication information, personal privacy [15] information, and other pieces of information. Due to the highly dynamic nature of the IoV, the onboard software system changes and updates frequently, so the vehicle must ensure the reliability of the source of the updates and information it receives. Otherwise, severe failure can occur in some cases.

2.6. Exclusive Attack. Most applications in IoV, such as traffic information, weather conditions, and navigation, rely on location information. Incorrect or misleading location information can lead to accidents, financial losses, and even life-threatening situations. The identity of a competent, connected vehicle is legal, but an attacker can launch an attack by forging the location, which is rare in a traditional network. Literature [16] describes detailed types of VeReMi: constant attacker, constant offset, random attack, random offset, and eventual stop.

Of course, the blockchain also has many security problems, such as a 51% attack. In [2], the paper proposes a regional blockchain. On the premise of ensuring the stability of the blockchain, by controlling the number of vehicles, malicious vehicles, and message transmission, several control parameters such as time and puzzle calculation time make the attack success rate reach 51%.

Unlike the traditional network's deep and hierarchical defense system, it urgently needs us to introduce new technologies and models to build a security system due to the particular requirements of decentralized and high mobility of computing, storage, and other resources.

3. The System Model of Blockchain-Based IoV (BIOV)

Most scenarios in IoV are real-time and mobile, generating and exchanging large amounts of data [17]. In particular, many of the classic technology centralized security technologies are unlikely to be suitable for scenarios. Therefore, blockchain can provide a large number of innovative solutions for most application scenarios. So, on the other hand, integrating blockchain into the Internet of Vehicles not only improves the security, privacy, and trust of the Internet of Vehicles but also enhances the performance and automation of the system. To sum up, to accommodate flexibility and handle large amounts of data, we should combine blockchain technology with the Internet of Vehicles. This section will focus on the system model of BIOV.

According to the communication entities in the IoV system, Hu et al. [18] divided IoV into three levels: vehicle-mounted communication nodes (VCNs), roadside

communication nodes (RCNs), and blockchain cloud platform. VCNs are mobile nodes installed on the vehicle, responsible for communication with other vehicles. However, the calculation and storage capabilities of VCNs are relatively weak. RCNs are fixed nodes installed on a roadside base station, responsible for promptly sharing information with other nodes in the network, but have strong computing and storage capabilities. Therefore, RCNs are the consensus information nodes of the Internet of Vehicles. The blockchain cloud platform will store all data on the Internet of Vehicles. Ma et al. introduced cloud computing in [19] and proposed security, privacy protection, and decentralized car networking architecture. The architecture uses blockchain and delegated PoS and consists of vehicles, sensors, actuators, RSU, and cloud computing nodes. RSU is the central blockchain storage node in this architecture. The cloud computing node is responsible for backing up and storing data such as the blockchain. The architecture contains two different subchains, namely, InterChain and IntraChain, which provide users with flexibility in access control. InterChain is responsible for sharing information between vehicles, roadside equipment, and other infrastructures. IntraChain maintains the communication between sensors, drivers, and personnel in the vehicle.

In [18, 19], roadside units (RSU/RCN) serve as nodes of the blockchain, but there is no mention of how to plan the deployment of roadside units. Therefore, such solutions require mathematical modeling of roadside units and the scale of roads and blockchains in natural environments. Therefore, Gao et al. [20] combined fog computing and SDN and proposed new system architecture. The fog computing platform comprises roadside units, vehicles, base stations, and other infrastructures. The SDN controller implements resource allocation, mobility management, and rule generation. SDN plane data consists of the vehicle, BS, and RSU, whose primary duty is to collect and forward the data to the quantization control plane. The control plane is composed of an SDN controller, RSU, and blockchain and determines the flow rules of the network. The nodes in the blockchain are composed of an authentication server, an access controller, a data management server, and a policy management server. Their functions are registration authentication, access control, data, and security policy management. This model gives a new solution. RSU no longer holds the nodes of the blockchain. However, the coordination and management between node servers is still a problem to be solved.

Lin et al. [21] combined blockchain, DRL (deep reinforcement learning), and spatial crowdsourcing technology and proposed a spatial crowdsourcing system (DB-SCS) based on deep reinforcement learning and blockchain. The DB-SCS system consists of three layers: the spatial crowdsourcing layer, the blockchain layer, and the DRL layer. In the spatial crowdsourcing layer, hierarchical task management and people management modules divide tasks and people into different security levels and manage them differently in task release and assignment. The blockchain layer uses the blockchain as a distributed server. Building a private blockchain based on Hyperledger Fabric [22, 23] by storing crowdsourcing tasks in the form of transactions on the

blockchain overcomes the single point of failure problem of traditional crowdsourcing. Using the subchain mechanism and decentralized server module, it is responsible for constructing different subblockchains for tasks of varying security levels, as a decentralized server to manage the functions and staff on the subblockchain. The fusion of DRL, deep learning and reinforcement learning, and the consensus algorithm of dynamic selection of blockchain realize spatial task allocation and blockchain performance improvement.

While the researchers are researching the BIoV model with the entity as the center, some researchers are also studying with the data. Gao et al. [20] and others divided BIoV from bottom to top: perception layer, communication layer, blockchain middle layer, computing layer, and application service layer. The framework integrates blockchain technology from the third layer. The communication layer realizes information interaction between vehicles through Bluetooth, VANET, and so on and uploads data to the blockchain middle layer through cellular networks, wide area networks, and other network services [24]. In the communication layer, authentication services based on blockchain ensure the reliability of communication objects. At the same time, hashing and other digital signature verification technologies safeguard the integrity of information. The middle layer of the blockchain provides essential blockchain application services. They deploy in the computing layer of the blockchain's all-node mining machine. It uses the public key address as a credential to encrypt and store information to ensure the confidentiality of data. The application layer uses smart contracts to force applications and underlying drivers to upgrade, avoiding intrusion caused by software and hardware vulnerabilities and ensuring that hackers cannot embed malicious code during updates. The network model proposed by Liu et al. [25] integrates blockchain technology into each layer, namely, data, network, artificial intelligence, application, and business. The network layer consists of the network coordination module and the P2P network sublayer of the blockchain. The AI layer, composed of the blockchain consensus sublayer and vehicle-oriented computational analysis services, includes the blockchain consensus protocol that runs on this layer. The smart contract sublayer of the blockchain runs in the application layer; the blockchain-dense sublayer rewards the first miner who provides a valid PoW using a digital token. Smart contracts are a set of predefined protocols that all peers operate in a blockchain-based system to meet specific service requirements. The business model of the Internet of Vehicles, data transaction business, and debt business constitute the business layer.

Jiang et al. [26] divided the blockchain data on the Internet of Vehicles into five categories: vehicle management blockchain data, automobile factory blockchain data, user privacy (audio and video) blockchain data, vehicle-insurance-purchase-blockchain data, and common things blockchain data. The blockchain nodes on the Internet of Vehicles are divided into five types of nodes: senior management nodes, vehicle monitoring nodes, privacy (audio and video) monitoring nodes, insurance nodes, and general transaction nodes.

We can compare the architectures studied in the above literature as shown in Table 1. With the further integration of blockchain and IoV, the performance requirements of blockchain will become higher and higher. A single chain may not meet the needs of multiservice scenarios in IoV, and a single chain will increase system load, resulting in more significant latency and computing costs.

To sum up, the architecture design of the BIoV system should follow the following principles:

- (i) Availability and fault tolerance principle: when some nodes are offline, vehicles on the road communicate continuously
- (ii) Easy deployment: using existing infrastructure saves money and time; communication with existing infrastructure achieves availability goals
- (iii) Adaptability: the network framework can be applied to various scenarios of vehicle driving environment and can meet the growing requirements of vehicles, data, and safety
- (iv) Security: it can guarantee the communication and data security of the Internet of Vehicles

4. Security Technology of BIoV

This section will focus on blockchain-based security technologies for the Internet of Vehicles. By keyword retrieval of Internet of Vehicles, blockchain, security technology, and so on, we searched relevant literature since 2010, manually screened the title and abstract of the paper, conducted corresponding screening according to the quality of the article, and sorted out and analyzed as many high-quality papers as possible. In Figure 1, the security technologies are classified based on the research of the papers we reviewed and concerning the existing Internet of Vehicles defense technologies.

4.1. Identity Authentication. Anonymous authentication is a commonly used technology to protect vehicle identity and privacy in IoV [27]. Vijayakumar et al. [28] proposed a two-factor authentication and key management mechanism for secure data transmission in virtual networks, which provided a high level of security for the vehicle side of virtual networks. Azeez et al. [29] designed an efficient anonymous authentication mechanism with conditional privacy protection for virtual networks to reduce the storage overhead of vehicles and anonymous roadside certificates. Karati et al. [30] introduced a new identity-based signature encryption mechanism suitable for low-bandwidth communication. In [31], Zhang et al. proposed an effectively distributed aggregation-privacy-protection-authentication protocol. Islam et al. [32] proposed an effective password-based conditional privacy protection authentication and group key generation protocol. The above literature relies on a management center with a preestablished trust relationship with the vehicle.

Fromknecht and Velicanu [33] presented a decentralized PKI (Public Key Infrastructure) authentication system based on blockchain and Bitcoin. This paper builds CertCoin on

TABLE 1: Comparison of architecture of BIoV.

Classification of models	Literature	Key technologies used in the model	Strengths/weaknesses
Entity-centric model	[10]	Blockchain	RSU acts as a blockchain node, but the scale and deployment issues of nodes are not resolved The problem of coordination between nodes has not been solved The performance of the blockchain is improved, but the computing power and throughput performance requirements are increased
	[11]	Cloud computing and double-chain structure	
	[12]	SDN, fog computing, and blockchain	
	[13]	Blockchain, deep learning, and spatial crowdsourcing	
A model centered on the data life cycle	[2, 16]	The communication layer, the computing layer, and the application layer are integrated with the blockchain technology	Integrate data and blockchain to varying degrees, but the management and performance of the system bring great challenges
	[17]	Blockchain is incorporated into every layer of the model	
	[18]	Five types of data correspond to five subchains	

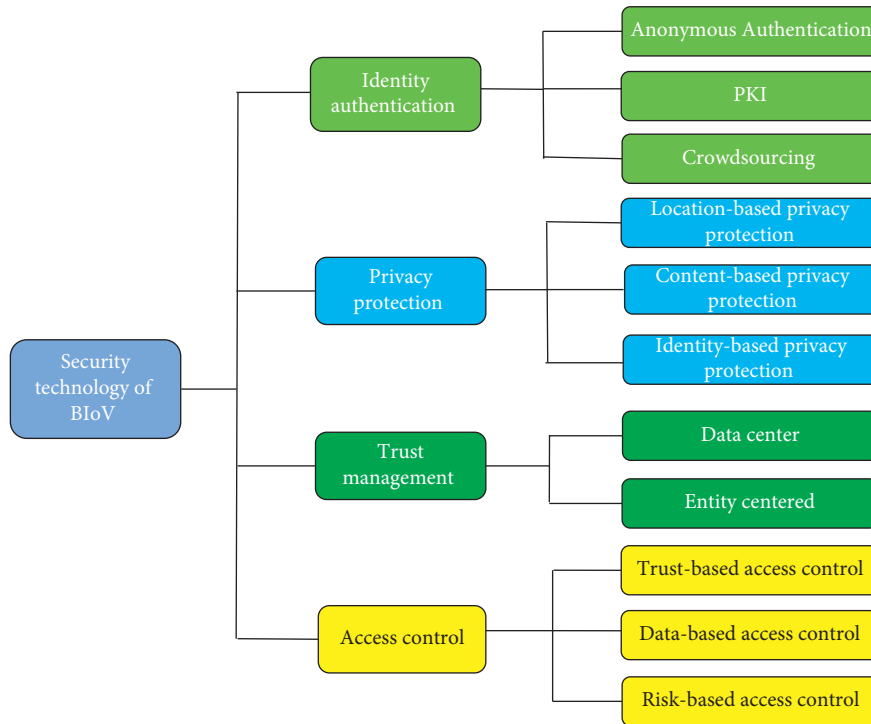


FIGURE 1: Security technology categories of BIoV.

top of Namecoin, whose core idea is to maintain a public ledger of a domain and its related public keys. It also supports domain name registration, domain name public key update, and authentication and provides revocation and restoration of the secret key. In addition, an accumulator is also used to reduce the storage of CertCoin.

Maria et al. [34] designed an anonymous authentication and switching authentication scheme. First, trusted authority (TA), RSU, vehicle, and blockchain network constitute the system. Then, system initialization, TA registration, anonymous authentication, and switching anonymous authentication comprise blockchain-based authentication. The Merkle Hash Tree (MHT) is the real-time authentication record. The blockchain server serves as an auxiliary for anonymous switching authentication. This

scheme also can be used as vehicle illegal information tracking and traceability.

Yao et al. [35] firstly proposed a noninteractive anonymous cross-data center authentication mechanism. The instrument's flexibility is that the vehicle can decide when to revalidate and change the pseudonym and how often to verify and change. Blockchain-assisted Lightweight Anonymous Authentication (BLA) begins by registering the vehicle's OBU and service manager (SM). Then, SM can cooperate with RSU to complete the identity authentication. SM broadcasts the authentication results and writes the authentication results into the blockchain through the PBFT (Practical Byzantine Fault Tolerance) consensus algorithm. When the vehicle moves to the next RSU or new SM area, it does not need to authenticate again. This solution eliminates

the interaction between the vehicle and SM and reduces the communication overhead.

Noh et al. [36] discussed a distributed message authentication scheme based on blockchain. First, the RTA (root trusted authority) acts as the management system to issue the certificates of the vehicles entering the network. Vehicles need to verify the driver's biometric information before broadcasting messages. Other vehicles receive the broadcast message for authentication. After receiving the message within a certain period, the local TA generates a block according to the PoW consensus and verifies the block through the PBFT consensus. It guarantees anonymity and dispersion of broadcasting information. In particular, it enables vehicles to authenticate messages efficiently and distribute them.

Zheng et al. [37] proposed an access authentication system based on blockchain in a VANET environment. The system provides a trusted communication environment for intelligent vehicles and maintains anonymity without revealing the user's true identity. Secure access between vehicles and roadside units reduces reliance on authority centers and reduces the burden of vehicle identification. To prevent the spread of internal vehicle forged messages, this paper also designs a secure distributed transaction storage scheme based on blockchain, which can effectively protect the transaction information from attacks while tracking malicious vehicles.

To sum up, identity authentication is an essential part of the IoV. Vehicles should be registered and assigned keys by a unified authority before joining the network. To avoid a single point of failure, we need to implement blockchain through consensus or smart contracts, credit mechanisms between vehicles, or RSU. The role of blockchain is to store, update, and manage secret keys or certificates. In Table 2, we can compare the application of blockchain in the identity authentication scheme of the Internet of Vehicles mentioned above.

4.2. Privacy Protection. IoV uses V2X interconnectivity such as V2V (Vehicle-to-Vehicle), V2R (Vehicle-to-Road), V2I (Vehicle-to-Infrastructure), and V2P (Vehicle-to-Person) to create a social network with intelligent objects as participants. V2X has led to the existence of vehicle social networks (VSNs). According to literature [39], VSN is divided into three layers: social network, vehicular social networks, and vehicular networks. The data sharing message of the social network includes the personal information of the car owner and the motion status of the vehicle. For example, the leakage of location privacy will seriously affect the user's identity privacy. It is precise because vehicle safety is closely related to the owner's daily life and work; privacy leakage will affect his everyday life and even affect his life and property safety. Therefore, privacy protection on the Internet of Vehicles environment is urgently needed. Butt et al. [40] pointed out that the role of privacy management becomes crucial in SIOV as data is collected and stored at different layers of its architecture. The author analyzes the privacy issues and factors that need to be considered in

privacy protection in the SIOV environment from different perspectives, such as personal privacy, behavior and action, communication, data, image, thought and feeling, location, and space association. In addition, the literature analyzes existing blockchain-based privacy protection methods. The difference is that we divide them into three types according to the objects of privacy protection: privacy protection technology based on location, content, and identity.

Qian et al. [41] proposed a privacy-aware content caching architecture based on blockchain. In this architecture, blockchain technology completes and records transactions. After a consensus mechanism finishes, transactions are written into blocks, thus solving the problem of privacy data disclosure in content caching.

Lin et al. [21] proposed a spatial crowdsourcing system (DB-SCS) based on deep reinforcement learning (DRL) and blockchain. The authors integrate deep reinforcement learning (DRL) and blockchain into the spatial crowdsourcing process of SDN-IOV applications. In DB-SCS, to protect the privacy of tasks in task assignment and publishing, two methods are proposed: hierarchical task classification and management strategy based on multiblockchain and task assignment scheme based on DRL.

Xu et al. [42] proposed a remote authentication model based on a privacy protection blockchain called RASM (remote authentication security model) for intelligent vehicles in the V2X network. This security model aims to enhance privacy security while ensuring decentralization, traceability, and nonrepudiation. RASM consists of two main steps. The first step is identity authentication; vehicles share their trusted identity to the blockchain network as evidence. In the second step, the vehicle will calculate and estimate the criteria used to decide. Finally, the authors tested the scheme in a real network environment, and the success rate of 97.09% proved that the system could effectively improve the privacy security of V2X vehicles.

A conditional Privacy Protection Statement Protocol (BTCPS), which contains three entities, vehicle, trusted institution, and RSU, was proposed by Liu et al. [43]. The protocol has two parts: the anonymous aggregation vehicle announcement protocol and privacy protection. The second step is the TM model based on blockchain. The trust value mechanism of direct and indirect trust realizes message synchronization and prevents abnormal vehicles from spreading false messages.

Luo et al. [44] introduced blockchain to realize location privacy protection of vehicles based on location services in IoV. This solution solves the distributed K-anonymous privacy protection technology that cannot detect malicious vehicles and sensitive location privacy leakage. In addition, the scheme considers the reliability of the vehicles and realizes the coordination between the vehicles. The scheme also includes a data structure to make trusted records of vehicles publicly available, which can detect malicious vehicles.

Different from K-anonymous privacy protection technology, Feng et al. [45] proposed a trusted stealth area construction scheme based on trust, called TACA, to protect vehicle location privacy, which is similar to the idea of stealth

TABLE 2: Comparison of identity authentication.

Literature	Registration authority	Functions of RA	Functions of blockchain	Method
[30]	Namecoin	Public key signature information	Publish, update, and validate	Merkle tree
[34]	The offline registration	Random number and public key	Validate	RSU collaboration
[35]	AD	SM area management	Alliance chain validation	Consensus algorithm
[36]	RTA	Public-private key for the vehicle and system key K	Validate	PoW and PBFT
[38]	CA	A certificate and two special hash functions	RSU	Pseudonyms and hashes

area [44]. In addition, with the assistance of edge computing and blockchain, the RSU can quickly evaluate the trust value by using the trust data gathered from the blockchain. The scheme proposes that multiple anonymous persons in the adjacent vehicle area are selected to construct the stealthy region in a cross-region manner. This scheme can effectively protect the location privacy of the vehicle and avoid the leakage of RV's (request vehicle) request content and LSP's (Location-Based Service Provider) service results during transmission.

Akhter et al. [46] proposed a multilevel privacy protection authentication protocol based on blockchain, which includes two certification centers. The Global Certification Center (GAC) is responsible for storing all vehicle information. The Local Certification Center (LAC) maintains a block to realize fast switching between clusters within the vehicle. In addition, the paper also puts forward that a tree can represent the blockchain-based authentication system. At the top level, the GAC stores all vehicle information (public and private keys, etc.). All vehicles must be registered with the LAC before a road permit. The LAC is responsible for physically verifying each vehicle and generating a public-private key pair. All LACs maintain a blockchain called an LABC by storing only information about locally registered vehicles, storing only public keys and vehicle types in the second layer of the tree structure. All CHs in the same state are members of LABC (as the third level of the tree), thus obtaining a list of all locally registered vehicles. Whenever a new vehicle approaches and requests to join the cluster, the CH can verify the vehicle's authenticity. Communication between the blockchain and its members is encrypted using the RSA-1024 digital signature algorithm. The author implements the authentication protocol in virtual machines and tests the computer, storage, and propagation costs in the authentication process.

To sum up, we compare the above literature on privacy protection, as shown in Table 3. Privacy protection mainly focuses on two aspects: privacy protection of the Internet of Vehicles social network and privacy protection of vehicle location. Privacy protection focuses on two parts: the privacy protection of a social network of Internet of Vehicles and the privacy protection of the vehicle location. The privacy protection of social networks mainly focuses on protecting vehicle identity information, transaction content, and so on. Location privacy protection especially involves vehicle tracking and location and service provision. However, for location privacy protection, conditional privacy protection in the case of information sharing needs to be established to

ensure the regular use of Internet of Vehicles location services and other applications.

4.3. Trust Management. Most existing trust management methods focus on collecting various pieces of evidence and analyzing the historical behavior of nodes to evaluate their trustworthiness of nodes. Unlike the object-oriented foundation, trust models can also be divided into three types [38, 47]: message-centric, entity-centric, and hybrid or composite models. Likewise, deployment strategies for trust management can be classified into centralized and decentralized types. Trust in the Internet of Vehicles is based on the trust value gained by the vehicle's past behavior (reputation) and neighbors' opinions on the messages broadcast by the warning vehicle in the event to realize the vehicle's importance. Trust management can facilitate peer incentives that perform well and achieve good trust scores. The system also punishes dishonest or misbehaving peers. When misbehavior exceeds a certain threshold, trust scores are low, and trust is revoked. Therefore, trust management has profound significance for the security of the Internet of Vehicles and is also the basis for identity authentication and access control.

Yang et al. [48] designed a trust model based on the data center category and used blockchain to conduct decentralized trust management for vehicle networks. They used a Bayes reasoning model to assess the credibility of messages received from neighbors. The vehicle periodically uploads the rating for each original vehicle generated to an adjacent RSU. The RSU calculates the offset of the confidence value, formed into blocks, which finally add to the blockchain that the RSU plans to hold. Through this strategy, the RSU maintains a dependable and consistent blockchain.

Lu et al. [15] adopted a blockchain-based anonymous reputation system (BARS) to implement suggestions to build trust and protect privacy. BARS systems include certificates to protect vehicle privacy, certificate management, certification bodies (CAS), law enforcement agencies (LEA), and vehicles and RSUs. There are three blockchain structures in BARS: MesBC (blockchain for messages) for continuous proof of the reputational evaluation, CerBC (blockchain for certificates) for all certificates issued, and RevSC (blockchain for revoked public keys) for revoked public keys. BARS uses extensive blockchain technology to achieve transparency, conditional anonymity, and robustness. The reputation valuation algorithm objectively reflects the message's credibility.

TABLE 3: Comparison of privacy protection.

Literature	Object	Method	Superiority
[41]	Content	Cognitive engine	Flexible short response time
[42]	Content	Software-defined networking, deep reinforcement, and learning spatial crowdsourcing	High throughput and low overhead
[43]	Identity	Remote authentication model	Trace
[44]	Identity	Conditional privacy statement protocol	Trust management method preventing forged messages
[45]	Location	Trust management method based on Dirichlet distribution	Detection of malicious vehicles
[46]	Location	Construction of trusted stealth region based on trust mechanism	Limited computing time and communication costs
[38]	Identity	Cluster-based MAC authentication protocol (ACB-MAC)	High throughput and lower latency

Javaid et al. [49] proposed a data sharing and trust management system for the BIoV. This document initially uses the Physical Nonclone Function (PUF) function to generate and assign a unique vehicle identifier. Then, two smart contracts are designed: one for the interaction between RSU and smart vehicle, and the other for the storage and retrieval of data from the blockchain, to establish distributed trust management and realize safety data sharing while protecting privacy. In [50], the author introduces the PoW dynamic mechanism to expand the traffic flow generated by vehicles and designs the data structure of the vehicle's blockchain in detail. The diagram attributes to each vehicle user a blockchain account with a 20-byte address similar to Bitcoin and Ethereum. The operation of the address size protocol is divided into two phases: the configuration phase for vehicle registration and the data transfer phase for communication between vehicles. Smart contracts with PUF, certificates, and dPoW consensus algorithms constitute the blockchain's IoV confidence management system.

Singh et al. [51] studied that smart contracts deployed through the CA/TA and that the USR was working in a distributed way to maintain a consistent vehicle confidential database and improve reliability, availability, and consistency. This paper introduces the concept of sharing blockchain, which uses an authoritative consensus mechanism, which can reduce the propagation delay of transactions and improve the throughput and efficiency of the whole system. In addition, the authors also introduce incentive strategies to help the vehicles participating in event detection obtain various services and pay incentives through the detection and accurate reporting of the actual event. The authors implemented the scheme in the private Ethereum blockchain and proved the feasibility of the framework by testing average throughput and runtime performance.

Han et al. [52] defined malicious behaviors and malicious RSUs of vehicles, then proposed a vehicle trust evaluation algorithm based on the hidden Markov Model (HMM), built Hyperledger Fabric, designed three smart contracts, and realized the functions of adding, updating, and querying data transactions. Finally, to solve the problem of malicious vehicles sending false information, the author builds a trust management model of a truck network based on blockchain, which improves the accuracy of malicious behavior detection.

In conclusion, in terms of trust management, blockchain technology has been fully integrated with IoV. The introduction of consensus mechanism, smart contract, incentive strategy, and the comparison of their technology applications shows in Table 4. At the same time, it also reflects the advantages of blockchain, a public distributed ledger, in terms of trust management, which can fully solve the problem of node trust in the Internet of Vehicles. However, we cannot ignore the cost of communication, computing, and storage. Therefore, we need to look at trust management solutions and do lightweight optimizations.

4.4. Access Control. With expanding scale in IoV, the amount of generated data is increasing exponentially. Secure systems must effectively control access to this information to protect the network from specific attacks (data analysis, tracking, etc.).

Sharma and Chakraborty [53] propose a system for vehicle data management that incorporates secure identity authentication, privacy protection, and access control. This system consists of a vehicle, a model, a chain, a registry, and a service provider. The vehicle can request information from the service provider, who adds the access request details, along with the permission status, to the blockchain as transactions.

Considering the need for both attribute-based data access control and location-based data access control, Jiang et al. [54] developed a location-based data access control scheme (LB-DAC) for vehicle networking. Data owners, data users, cloud storage servers, attribute permissions, location permissions, fog computing nodes, and blockchain systems are the seven entities defined within the LB-DAC scheme. Data owners can encrypt data and upload it to the cloud server under specific access control policies. Decryption can only occur if the vehicle's attributes and location meet specific requirements. As a result, the addition of fog nodes enables the positioning function. When the vehicle arrives at the designated area, the vehicle receives a location key. Additionally, it provides computing resources for decrypting vehicles. As a tamper-proof bulletin board, the blockchain is responsible for publishing public parameters of property permissions and location permits.

Mendiboure et al. [55] introduced SDN to improve the scalability of blockchain networks and shorten the

TABLE 4: Comparison of trust management schemes.

Scheme	Smart contract	Consensus algorithm	Incentive mechanism	Others
[48]	N	Y	N	Bayes reasoning model
[15]	N	Y	N	Reputation evaluation algorithm
[49, 50]	Y	Y	N	PUF
[51]	Y	Y	Y	Sharing blockchain
[52]	Y	Y	Y	HMM

authentication/access control/undo process. The authors defined three types of nodes in this paper: local nodes, which only involve the local blockchain subnet, used to authenticate/control the access of devices (vehicles, SDN controllers, and roadside devices) located in the geographical area; internal nodes, nodes involving two or more local blockchain subnets, enabling transitional verification/control of access across different geographic regions; global node: a node that contains both the global blockchain network and the local blockchain subnet. It retrieves information about each local blockchain subnetwork and updates the global status of the network. When the SDN controller attempts to connect to the vehicle, the blockchain node checks whether the current geographical area of the vehicle belongs to the area authorized by the controller; if not, the contact deny.

Liu et al. [56] introduced the edge-chain system and designed a dynamic access control model based on risk prediction, RPBAC, to secure access control of Internet of Vehicles devices. The blockchain network consists of vehicle nodes and roadside cells (RSUs), where the edge chain is on the RSU, and the vehicle node serves as the lightweight node. The RSU, as a full node and an edge node (edge service), provides access control services for the vehicle node. Blockchain is responsible for safe storage, the smart contract is responsible for automatic execution of the control strategy, and the intelligent control module is responsible for a wise decision. The intelligent management control module establishes the RPBAC model by introducing GAN. The RPBAC model obtains the behavior data of the requesting vehicle from the blockchain and receives the numerical matrix from the historical behavior through data preprocessing. As the input of GAN, the numerical matrix predicts the requested vehicle's risk level. The risk prediction model is built on TensorFlow 1.12.0 and coded by Python. The expected risk level, combined with the security requirements of the resource owner's vehicle, is used to assess the access rights of the requesting vehicle and generate the corresponding access control policies.

In addition, attribute-based encryption (ABE) is an encryption technique that can simultaneously achieve data confidentiality and access control, especially those ABE schemes with revocation functions. However, most of the existing revocable ABE schemes require nodes to update the private keys of all nonrevoked nodes during the update and withdrawal process. Therefore, the key update work may become a system bottleneck. Wang et al. [57] proposed a dynamic fine-grained access control scheme based on ABE. According to the vehicle's attributes, the message sender can determine which vehicles receive the message and revoke the

decryption authorization for some vehicles without updating all unrevoked keys, reducing computational delay and communication overhead.

In summary, research on blockchain-based IoV access control technology is still at an early stage. In combination with identity authentication and privacy protection technology, there are more access control methods. But there are few methods for application access control. In the later stage, the application access control table can be designed according to the size of the blockchain to realize the access control of the application.

4.5. Other Solutions. To speed up distributed key management in heterogeneous networks and improve efficiency, Lai et al. [58] adopted blockchain technology. The framework consists of two schemes, namely, a new blockchain-assisted key management scheme and a dynamic transaction collection scheme. In the key management scheme, the authors eliminate the central manager and introduce multiple security managers to play an essential role in the authentication and verification of the key transmission process. The processed records are stored on the blockchain and shared between the SMs. On the other hand, the dynamic transaction acquisition scheme enables the system to reduce the key transmission time of the blockchain network during the vehicle switching process, and the acquisition cycle can change dynamically according to different traffic levels.

On behalf of ensuring the security and traceability of data sharing in-vehicle networks, Kang et al. [59] proposed a reputation-based blockchain scheme. Two smart contracts, DSSC (a data storage smart contract) and ISSC (information sharing smart contract), are deployed on the blockchain. DSSC realizes secure data storage, and ISSC realizes the efficient data sharing function. The paper also cites subjective logic to construct the interactive individual reputation evaluation. The authors propose a three-component local view TWSL (three-weight subjective logic), which is different from traditional subjective logic (TSL). They also consider interaction frequency, event timelines, track similarity, and combine local opinions with recommendations to achieve accurate reputation management and high-quality data sharing. Chen et al. [60] built a data sharing system composed of a two-layer blockchain based on a new content-centered vehicle Internet data sharing model-Vehicle Naming Data Network (VNDN), which has emerged in recent years. At the bottom, we divide vehicles into groups of blockchains based on their mobility trend similarity or PBO (a private blockchain for OBUs). At the top level, a pre-selected RSU executes the consensus process. Assume that

all vehicles inclined to participate in the information sharing system are legitimate entities registered with a trusted institution. The authors also model the balance between demand and supply as a matching game. To encourage nodes to provide forward services, the authors propose a reputation management mechanism that combines negative and forward transaction records to improve the security of information interaction in VNDN.

Akhter et al. [61] proposed a blockchain-based secure cluster MAC protocol (SCB-MAC) based on the traditional IEEE802.11 standard, which defined the formation of the cluster, handshake mode, and transmission of specific and nonsecure messages in detail. Assume that all vehicles are equipped with the hardware and software resources needed to send and receive information, such as OBUs, sensors, a global positioning system (GPS). They can connect to high-speed Internet. A Certification Authority (CA) physically verifies all vehicles. The CA assigns a public and private key pair to each car. The CA is considered secure enough to protect the privacy of the vehicle. Select a cluster leader (CH) and others as cluster members (CM) in a centralized vehicle system. CH will handle all NSMT between CMs as an access point. Each cluster has a blockchain to store secure messages. All CMs (including CH) are complete nodes, and anyone can initiate a transaction in a specified blockchain to notify of an emergency. The vehicle will sign the message with its private key to confirm its identity and ensure nonrepudiation. The blockchain server will check the authentication, generate a block from the transmission, and broadcast it to all members.

This section examines security solutions beyond identity authentication, privacy protection, trust management, and access control. These solutions only explore security issues at a specific point on the Internet of Vehicles, such as reputation-based data sharing, without considering privacy protection while considering data sharing. Therefore, we suggest that we take full advantage of the technical characteristics of IoV and blockchain and solve the security problems of the Internet of Vehicles through the IoV architecture and technology innovation of the integrated block.

5. Security Analysis Methods and Performance Parameters in BIoV

5.1. Security Analysis Methods. Based on thoroughly investigating blockchain-based IoV security technology in the last section, we analyzed that each protocol and scheme's simulation environment and analysis methods differed. This section focuses on security analysis methods and performance parameters in BIoV.

5.1.1. Informal Safety Analysis. Informal security analysis refers to the theory or process analysis of the following security elements according to the characteristics of security protocols proposed in this paper. Table 5 shows the comparison of relating schemes.

Bidirectional authentication: in the designed certification process, certification entities are for mutual certification.

Key management: in the scheme designed in this paper, after mutual authentication and key protocol are completed, the secret key is generated, stored, and revoked, and this forms the life cycle management of the private key

Privacy protection: in schemes, protocols, and other processes, it is necessary to consider preventing the disclosure of information such as original identity and how to share sensitive information (such as anonymity and location)

Resist attacks: according to the design of the agreement and scheme, it is necessary to consider resisting the man-in-the-middle attack, DOS attack, and other kinds of attacks proposed in Section 2

5.1.2. Formal Safety Analysis Methods. The formal security analysis method is proved by mathematical theorem. First, establish the theorem. Secondly, the popular security verification tool ProVerif [66] verifies the security of the proposed authentication protocol. ProVerif is an automatic formal verification cryptographic protocol tool based on the Dolev-Yao model developed by Bruno Blanchet. It is implemented in the Prolog language. It can describe a variety of cryptographic primitives, including shared key and public key cryptography (encryption and digital signature), hash functions, and Diffie-Hellman key exchange protocols. It can specify rewrite rules and equations for input languages, such as applying PI calculus or the Horn word. The authentication protocol used for authentication is divided into three parts [67]: (1) declaring encryption primitives, (2) defining processes on the primary process and a single entity as child processes, and (3) instantiation child processes using the immediate process. When using the ProVerif tool to verify the cryptographic protocol, this tool will give a corresponding attack sequence if the protocol has vulnerabilities. ProVerif can prove the following attributes: confidentiality (the adversary does not have access to the secret), authentication and its more general counterpart, high secrecy (the adversary does not see the difference when the secret value changes), and only equivalence between processes with different terms. Table 6 lists a comparison of formal safety analysis methods in the literature.

5.2. Performance Evaluation Characteristic Parameters and Comparison. We summarize the blockchain types and performance evaluation parameters involved in the literature, as shown in Table 7. We can see that, by evaluating the methods proposed in the literature in a blockchain, in addition to the regular communication overhead and computational overhead, the researchers also assess the storage overhead.

(1) Communication overhead: this parameter is the maximum packet size required for protocol

TABLE 5: Comparison of informal safety analysis methods.

Security characteristics	[62]	[63]	[64]	[65]
Bidirectional authentication	Y	Y	Y	N
Key management	Y	Y	N	Y
Privacy protection	PFS/PBS	Y	N	N
Resist attacks	Man-in-the-middle attack	Man-in-the-middle attack	DOS attack, physical attack, and man-in-the-middle attack	Resist cyberattacks

TABLE 6: Comparison of formal safety analysis methods.

Literature	[25]	[35]	[53]	[55]	[58]
Mathematical theorem proof	Y	Y	N	Y	N
ProVerif	N	N	Y	Y	Y

TABLE 7: Blockchain simulation and parameters.

Literature	Simulation tools	Blockchain	Parameters for performance evaluation
[21]		Hyperledger Fabric 1.2	Storage overhead and computational overhead
[35]	Cygwin	NO	Computational overhead and communication overhead
[51]		Ethereum blockchain	Computational overhead and communication overhead
[61]	Truffle framework	Ethereum blockchain	Storage overhead delay

transport. Literature [48] points out that there are two kinds of data, namely, secure and nonsecure messages, transmitted through a wireless channel in the vehicular network. Safety messages are triggered by specific road-related events and broadcast by the vehicle; the packet size of the message is set to 800 bytes. Unsafe data generated by a car are accumulated in a certain period, packaged into a packet, and uploaded to a nearby RSU. The size of the nonsecure message packet is usually more significant than the size of the secure message. In literature [50], the size of the blockchain data packet is 512 bytes, and the size of the application data packet is 64 bytes.

- (2) Computational complexity: the computational complexity is related to the algorithm used by the protocol or scheme. We can define the algorithm complexity involving signature, verification, encryption, and decryption in the process as $O(\text{Sig})$, $O(\text{Sig})$, $O(\text{Enc})$, and $O(\text{Enc})$ functions. We can compare literature [44] and literature [45], as shown in Table 8.

From the above comparison, we can see the location privacy protection scheme combined edge computing and RSU adopted in the literature [45] can quickly evaluate the trust value by using the trust data gathered from the blockchain. We want to protect vehicle location privacy while reducing computing time and communication costs. Of course, literature [44] strengthens the reliability of vehicles by analyzing various requirements of requesting and cooperating vehicles.

- (3) Decentralization: quantitative decentralization refers to the degree of decentralization of the system, and it can also judge the influence of system modification on the degree of decentralization. We can design and optimize algorithms and frameworks to maximize

decentralization. In [50], the Gini coefficient $g_{(\lambda)}$ is used to measure the dispersion of the proposed protocol by considering the geographical location distribution of miners' nodes. The Gini coefficient is in $[0, 1]$, where 0 represents complete dispersion and 1 represents total concentration. Therefore, the more dispersed or uniform the geographic distribution of miner nodes is, the closer the coefficient is to 0. In this paper, $\lambda(x)$ is used to express the geographical distribution density of RSU, and the Gini coefficient $g_{(\lambda)}$ can be expressed as

$$g_{(\lambda)} = \frac{\int_a \int_a |\lambda(x) - \lambda(y)| dy dx}{\int_a \int_a \lambda(x) dy dx} = \frac{\int_a \int_a |\lambda(x) - \lambda(y)| dy dx}{2M}, \quad (1)$$

where a is the area of the two-dimensional coordinate (x, y) of the geographical location of RSU and the distribution density of $\lambda(x)$ in this area.

- (4) Delay: the time required for the successful transmission of a message [46]. Then, the average delay $E[D]$ can be expressed as

$$E[D] = E[T_{\text{interval}}] - \frac{P_{f\text{drop}}}{1 - P_{f\text{drop}}} * E[T_{\text{drop}}]. \quad (2)$$

Among them $E[T_{\text{interval}}]$ represents the average time interval between two successful packets received, $P_{f\text{drop}}$ shows the packet loss probability, and $E[T_{\text{drop}}]$ expresses the average packet loss time.

Communication delay is an important indicator to judge whether the technical security solution of the Internet of Vehicles is efficient. The most common simulation indicators: the same method evaluates the change of the communication delay with the number of nodes to determine the

TABLE 8: Comparison of computational complexity.

Process of [45]	Computational complexity	Process of [44]	Computational complexity
Position verification	O (1)	Verification	O (sig)
Cross-regional trust stealth zone construction	O (1)	Request cooperative signature	O (sig)
Restore key and verify integrity	O (Enc)	Returns response	O (sig) + O (Enc)

scalability of the scheme; the comparison of the communication delay between different ways reflects the efficiency of the method.

6. Summarization and Prospect

Through the above discussion on various aspects of blockchain-based IoV technology, security and privacy issues in IoV applications have focused on people's attention. We can enhance decentralized privacy protection, traceability, and other types of security by integrating blockchain technology. The research achievements in identity authentication, privacy protection, trust management, access control, and so on have been made. However, the following problems remain unresolved. However, the following issues remain unresolved: (1) development of a blockchain-based IoV security framework, which is different from the traditional IoV network architecture. We can use existing infrastructure to build IoV systems at maximum cost savings; (2) studying new blockchain models. The model addresses current challenges such as growing nodes, ledger, and data, reducing complexity and latency, and increasing scalability; (3) strengthening the control layer. This layer mainly uses intrusion detection and attack mitigation control. These methods require numerical and theoretical analysis and can keep the network running in the face of errors, emergency demand outages, or physical attacks; (4) studying lightweight blockchain. The important limitations of smart contracts and consensus mechanisms are computing power, communication, and energy consumption; moreover, with the increasing number of vehicles, there is a lot of data transmission and storage consumption. Therefore, we should design a lightweight blockchain-based IoV framework or lightweight authentication and privacy protection protocols; (5) combination with existing new technologies. Blockchain can be combined with edge computing to enhance data analytics and improve the security of nodes on the Internet of Vehicles. Blockchain can also be combined with deep learning to build risk prediction models and improve access control security for Internet of Vehicles systems. Blockchain can also be combined with SDN and AI technologies to improve the transparency of the control plane. Therefore, the significance of the research work carried out in this paper is to summarize, classify, and discuss the existing blockchain-based Internet of Vehicles security technology, grasp its development direction, summarize verification and effective evaluation methods, and provide direction and method guidance for the following research work.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the following projects: (1) the Graduate Research Innovation Project of Jiangsu Province, China (Grant no. KYCX21_3087); (2) the National Natural Science Foundation of China (Grant no. 61771265); (3) the Key Science and Technology Foundation of Nantong (Grant no. MS22021034).

References


- [1] R. Shrestha, S. Y. Nam, R. Bajracharya, and S. Kim, "Evolution of V2X communication and integration of blockchain for security enhancements," *Electronics*, vol. 9, no. 9, p. 1338, 2020.
- [2] R. Shrestha and S. Y. Nam, "Regional blockchain for vehicular networks to prevent 51% attacks," *IEEE Access*, vol. 7, pp. 95033–95045, 2019.
- [3] S. Xie, Z. Zheng, W. Chen, J. Wu, H.-N. Dai, and M. Imran, "Blockchain for cloud exchange: a survey," *Computers & Electrical Engineering*, vol. 81, Article ID 106526, 2020.
- [4] P. Fraga-Lamas and T. M. Fernandez-Carames, "A review on blockchain technologies for an advanced and cyber-resilient automotive industry," *IEEE Access*, vol. 7, pp. 17578–17598, 2019.
- [5] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A new type of blockchain for secure message exchange in VANET," *Digital communications and networks*, vol. 6, no. 2, pp. 177–186, 2020.
- [6] T. Ali Syed, A. Alzahrani, S. Jan, M. S. Siddiqui, A. Nadeem, and T. Alghamdi, "A comparative analysis of blockchain architecture and its applications: problems and recommendations," *IEEE Access*, vol. 7, pp. 176838–176869, 2019.
- [7] T. Ali, A. Nadeem, M. Shoaib, M. Nauman, and A. Alzahrani, "Blockchain-based-vehicle-life-cycle-tracking-system," 2019, <https://www.researchgate.net/project/Blockchain-Based-Vehicle-Life-Cycle-Tracking-System>.
- [8] M. L. Chavez, C. H. Rosete, and F. R. Henriguez, "Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study," in *Proceedings of the 15th International Conference on electronics (2005), communications and Computers*, August 2010, Article ID 166e70.
- [9] P. Sharma and H. Liu, "A machine-learning-based data-centric misbehavior detection model for internet of vehicles," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4991–4999, 2021.
- [10] S. Bono, M. Green, A. Stubblefield, A. Juels, A. D. Rubbin, and M. Szydlo, "Security analysis of a cryptographically-enabled RFID device," *USENIX Security Symposium*, vol. 31, 2005.
- [11] Sumra, I. Ahmed, H. BinHasbullah, J. L. A. Manan, and I. Ahmad, "Classification of attacks in vehicular ad hoc network (vanet)," *International Information Institute (Tokyo)*, vol. 5, p. 2995, 2013.
- [12] S. Checkoway, D. McCoy, and B. Kantor, "Comprehensive experimental analyses of automotive attack surfaces," *20th USENIX Security Symposium*, USENIX Security, vol. 11, 2011.

- [13] R. Shrestha and S. Y. Nam, "Trustworthy event-information dissemination in vehicular ad hoc networks," *Mobile Information Systems*, vol. 2017, Article ID 9050787, 2017.
- [14] J. R. Douceur, "The sybil attack," *Peer-to-Peer Systems*, Springer, Berlin, Heidelberg, pp. 251–260, 2002.
- [15] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655–45664, 2018.
- [16] S. So, P. Sharma, and J. Petit, "Integrating plausibility checks and machine learning for misbehavior detection in VANET," in *Proceedings of the 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)*, pp. 564–571, ICMLA, Orlando, FL, USA, December 2018.
- [17] S. Chen, X. Zhu, H. Zhang, C. Zhao, G. Yang, and K. Wang, "Efficient privacy preserving data collection and computation offloading for fog-assisted IoT," *IEEE Transactions on Sustainable Computing*, vol. 5, no. 4, pp. 526–540, 2020.
- [18] 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. 139703–139711, 2019.
- [19] X. Ma, C. Ge, and Z. Liu, "Blockchain-enabled privacy-preserving Internet of vehicles: decentralized and reputation-based network architecture," in *Proceedings of the International Conference on Network and System Security*, December 2019.
- [20] J. Gao, K. O. B. Obour Agyekum, E. B. Sifah et al., "A blockchain-SDN-enabled internet of vehicles environment for fog computing and 5G networks," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4278–4291, 2020.
- [21] H. Lin, S. Garg, J. Hu, G. Kaddoum, M. Peng, and M. S. Hossain, "Blockchain and deep reinforcement learning empowered spatial crowdsourcing in software-defined internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3755–3764, 2021.
- [22] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: a survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, 2019.
- [23] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4298–4311, 2020.
- [24] F. Dai, H. Chen, Z. Qiang, Z. Liang, B. Huang, and L. Wang, "Automatic Analysis of Complex Interactions in Microservice Systems," *Complexity*, vol. 2021, Article ID 2128793, 2020.
- [25] K. Liu, W. Chen, Z. Zheng, Z. Li, and W. Liang, "A novel debt-credit mechanism for blockchain-based data-trading in internet of vehicles," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9098–9111, 2019.
- [26] T. Jiang, H. Fang, and H. Wang, "Blockchain-based internet of vehicles: distributed network architecture and performance analysis," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4640–4649, 2019.
- [27] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 2, pp. 760–776, 2019.
- [28] P. Vijayakumar, M. Azees, A. Kannan, and L. Jegatha 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, 2016.
- [29] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 9, pp. 2467–2476, 2017.
- [30] A. Karati, S. H. Islam, G. P. Biswas, M. Z. A. Bhuiyan, P. Vijayakumar, and M. Karuppiah, "Provably secure identity-based signcryption scheme for crowdsourced industrial internet of things environments," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2904–2914, 2018.
- [31] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 516–526, 2017.
- [32] S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy, "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs," *Future Generation Computer Systems*, vol. 84, pp. 216–227, 2018.
- [33] C. Fromknecht and D. Velicanu, "CertCoin: A NameCoin Based Decentralized Authentication System" 6.857 Class Project, 2014, <https://courses.csaail.mit.edu/6.857/2014/files/19-fromknecht-velicann-yakoubov-certcoin.pdf>.
- [34] A. Maria, V. Pandi, J. D. Lazarus, M. Karuppiah, and M. S. Christo, "BBAAS: blockchain-based anonymous authentication scheme for providing secure communication in VANETs," *Security and Communication Networks*, vol. 2021, Article ID 6679882, 11 pages, 2021.
- [35] Y. Yao, X. Chang, J. Mistic, V. B. Mistic, and L. Li, "BLA: blockchain-assisted lightweight Anonymous authentication for distributed vehicular fog services," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3775–3784, 2019.
- [36] J. Noh, S. Jeon, and S. Cho, "Distributed blockchain-based message authentication scheme for connected vehicles," *Electronics*, vol. 9, no. 1, p. 74, 2020.
- [37] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A traceable blockchain-based access authentication system with privacy preservation in VANETs," *IEEE Access*, vol. 7, pp. 117716–117726, 2019.
- [38] J. Zhang, "Trust management for VANETs," *International Journal of Distributed Systems and Technologies*, vol. 3, no. 1, pp. 48–62, 2012.
- [39] S. Kim and R. Shrestha, "Internet of vehicles, vehicular social networks, and cybersecurity," *Automotive Cyber Security*, Springer, Singapore, pp. 149–181, 2020.
- [40] T. A. Butt, R. Iqbal, K. Salah, M. Aloqaily, and Y. Jararweh, "Privacy management in social internet of vehicles: review, challenges and blockchain based solutions," *IEEE Access*, vol. 7, pp. 79694–79713, 2019.
- [41] Y. Qian, Y. Jiang, L. Hu, M. S. Hossain, M. Alrashoud, and M. Al-Hammadi, "Blockchain-based privacy-aware content caching in cognitive internet of vehicles," *IEEE Network*, vol. 34, no. 2, pp. 46–51, 2020.
- [42] C. Xu, H. Liu, P. Li, and P. Wang, "A remote attestation security model based on privacy-preserving blockchain for V2X," *IEEE Access*, vol. 6, pp. 67809–67818, 2018.
- [43] X. Liu, H. Huang, F. Xiao, and Z. Ma, "A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4101–4112, 2020.
- [44] B. Luo, X. Li, J. Weng, J. Guo, and J. Ma, "Blockchain enabled trust-based location privacy protection scheme in VANET," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 2, pp. 2034–2048, 2020.
- [45] J. Feng, Y. Wang, J. Wang, and F. Ren, "Blockchain-based data management and edge-assisted trusted cloaking area construction for location privacy protection in vehicular

- networks,” *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2087–2101, 2021.
- [46] A. F. M. S. Akhter and M. Ahmed, A. A. Shah, A. F. M. S. Shah, A. Anwar, and A. Zengin, “A secured privacy-preserving multi-level blockchain framework for cluster based VANET,” *Sustainability*, vol. 13, no. 1, p. 400, 2021.
- [47] S. A. Soleymani, A. H. Abdullah, W. H. Hassan et al., “Trust management in vehicular ad hoc network: a systematic review,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2015, no. 1, p. 146, 2015.
- [48] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, “Blockchain-based decentralized trust management in vehicular networks,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495–1505, 2019.
- [49] U. Javaid, M. N. Aman, and B. Sikdar, “DrivMan: driving trust management and data sharing in VANETs with blockchain and smart contracts,” in *Proceedings of the 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, pp. 1–5, Kuala Lumpur, Malaysia, May 2019.
- [50] U. Javaid, M. N. Aman, and B. Sikdar, “A scalable protocol for driving trust management in internet of vehicles with blockchain,” *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11815–11829, 2020.
- [51] P. K. Singh, R. Singh, S. K. Nandi, K. Z. Ghafoor, D. B. Rawat, and S. Nandi, “Blockchain-based adaptive trust management in internet of vehicles using smart contract,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3616–3630, 2021.
- [52] L. Han, D. Han, and D. Li, “Behavior analysis and blockchain based trust management in vanets,” vol. 151, pp. 61–69, 2021.
- [53] R. Sharma and S. Chakraborty, “BlockAPP: using blockchain for authentication and privacy preservation in IoV,” in *Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–6, Abu Dhabi, UAE, December 2018.
- [54] M. Jiang, H. Wang, W. Zhang, H. Qin, and Xi Sun, “Location-based data access control scheme for internet of vehicles,” *Computers & Electrical Engineering*, vol. 86, Article ID 106716, 2020.
- [55] L. Mendiboure, M. A. Chalouf, and F. Krief, “A scalable blockchain-based approach for authentication and access control in software defined vehicular networks,” in *Proceedings of the 2020 29th International Conference on Computer Communications and Networks (ICCCN)*, pp. 1–11, Honolulu, HI, USA, September 2020.
- [56] Y. Liu, M. Xiao, S. Chen, F. Bai, J. Pan, and D. Zhang, “An intelligent edge-chain-enabled access control mechanism for IoV,” *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12231–12241, 2021.
- [57] T. Wang, L. Kang, and J. Duan, “Dynamic fine-grained access control scheme for vehicular ad hoc networks,” *Computer Networks*, vol. 188, Article ID 107872, 2021.
- [58] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, “Blockchain-based dynamic key management for heterogeneous intelligent transportation systems,” *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1832–1843, 2017.
- [59] J. Kang, R. Yu, X. Huang et al., “Blockchain for secure and efficient data sharing in vehicular edge computing and networks,” *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4660–4670, 2019.
- [60] C. Chen, C. Wang, T. Qiu, N. Lv, and Q. Pei, “A secure content sharing scheme based on blockchain in vehicular named data networks,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3278–3289, 2020.
- [61] A. F. M. S. Akhter, A. F. M. S. Shah, M. Ahmed, N. Moustafa, U. Çavuşoğlu, and A. Zengin, “A secured message transmission protocol for vehicular ad hoc networks,” *Computers, Materials & Continua*, vol. 68, no. 1, pp. 229–246, 2021.
- [62] R. Ma, J. Cao, D. Feng et al., “A secure authentication scheme for remote diagnosis and maintenance in internet of vehicles,” *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–7, Seoul, Korea (South), May 2020.
- [63] T. Alladi, S. Chakravarty, V. Chamola, and M. Guizani, “A lightweight Authentication and attestation scheme for in-transit vehicles in IoV scenario,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 14188–14197, 2020.
- [64] M. N. Aman, U. Javaid, and B. Sikdar, “A privacy-preserving and scalable authentication protocol for the internet of vehicles,” *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 1123–1139, 2021.
- [65] M. Wazid, P. Bagga, A. K. Das et al., “AKM-IoV: authenticated key management protocol in fog computing-based internet of vehicles deployment,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8804–8817, 2019.
- [66] B. Blanchet and V. Cheval, “ProVerif: Cryptographic protocol verifier in the formal model,” 2020, <https://prosecco.gforge.inria.fr/personal/bblanche/proverif/>.
- [67] B. Blanchet and V. Cheval, “ProVerif 2.00: automatic cryptographic protocol verifier, user manual and tutorial,” pp. 05–16, 2018, <https://bblanche.gitlabpages.inria.fr/proverif/manual.pdf>.

Research Article

Threshold Key Management Scheme for Blockchain-Based Intelligent Transportation Systems

Tianqi Zhou ¹, Jian Shen ^{1,2}, Yongjun Ren ¹ and Sai Ji ^{1,3}

¹School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing, China

²Cyberspace Security Research Center, Peng Cheng Laboratory, Shenzhen, China

³Suqian University, Suqian, China

Correspondence should be addressed to Jian Shen; s_shenjian@126.com

Received 2 July 2021; Revised 1 August 2021; Accepted 19 August 2021; Published 8 September 2021

Academic Editor: Shichang Xuan

Copyright © 2021 Tianqi Zhou et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Intelligent transportation systems (ITS) have always been an important application of Internet of Things (IoT). Today, big data and cloud computing have further promoted the construction and development of ITS. At the same time, the development of blockchain has also brought new features and convenience to ITS. However, due to the endless emergence of increasingly advanced types of attacks, the security of blockchain-based ITS needs more attention from industry and academia. In this paper, we focus on exploring the primitives in cryptography to guarantee the security of blockchain-based ITS. In particular, the authentication, encryption, and key management schemes in cryptography are discussed. Furthermore, we propose two methods for achieving the threshold key management in blockchain-based ITS. The proposed threshold key management scheme (with threshold t) enables various stakeholders to recover a secret if the number of participated stakeholders is at least t . It should be noted that the proposed threshold key management scheme is efficient and secure for multiple users in blockchain-based ITS, especially for the data-sharing scenario.

1. Introduction

Nowadays, Internet of Things (IoT) [1, 2] have experienced unprecedented development due to the widespread of big data and cloud computing [3]. Modern intelligent transportation systems (ITS) [4–7] have extensively benefited from IoT technology. At the same time, the development of blockchain [8, 9] has also brought new features and convenience to ITS. However, due to the endless emergence of increasingly advanced types of attacks, the security of blockchain-based ITS needs more attention from industry and academia. The problems in ITS, such as data origin authentication, reliability, and trustworthiness, are required to be solved. Note that the blockchain technology maintains the decentralized, distributed, and tamperproof properties [8], which can guarantee the security and reliability of ITS communication. Also, the security of ITS requires more attention and delicate design to prevent it from various attacks. Generally speaking, the security attributes of ITS

security mainly include confidentiality, integrity, consistency, and availability. Confidentiality means that the transmitted data in ITS will not be leaked and accessed illegally. Note that encryption is an effective method to protect the confidentiality of the transmitted data in ITS. Integrity means that the data in ITS will not be maliciously destroyed and deleted. Consistency means that the data in ITS meets the entity integrity. The auditing scheme in cryptography can be employed to protect the integrity and consistency of ITS. Availability means that if a user is authorized, she/he can access ITS. Undoubtedly, cryptography plays a vital role in protecting the security of ITS.

In recent years, cryptography has developed rapidly and has been widely used in various fields of the Internet and computers. Generally, cryptography can be divided into two parts: classical cryptography and modern cryptography. Classical cryptography is based on replacement and substitution methods, while modern cryptography is based on mathematics, computer, and communication science. The

main research topics of modern cryptography include information encryption, digital signatures, data integrity, and identity authentication. More precisely, the paper [10] published by Shannon marks the beginning of modern cryptography. In this paper, the concept of unconditional security was proposed. Based on this concept, one-time pad (OTP) [11] is unconditional security; that is, even if an attacker has unlimited computing resources, it is impossible to decipher the ciphertext encrypted by OTP. However, it is obvious that OTP is unrealistic since the OTP requires that the transmission channel is secure, which is impractical in reality. In addition, if one can transmit the secret for the OPT, why not she/he transmits the message of the same length? Although unconditional security drives the proposal of computational security [12], the computational security is the fundamental of modern cryptography.

Modern cryptography includes symmetric cryptography and asymmetric cryptography. The later is also known as the public key cryptography [13]. The pioneer work of the public key cryptography is the well-known Diffie–Hellman key exchange [14], which was proposed by Diffie and Hellman in 1976. After that, the RSA algorithm [15] was designed by Rivest et al. The security of RSA algorithm is based on the factoring problem. Since then, a large number of excellent research results have emerged in the field of public cryptography. In this paper, primitives in cryptography is explored and utilized for achieving ITS security. Specifically, the threshold key management scheme is designed based on the (t, n) threshold secret sharing, which is an efficient and secure cryptography primitive.

The rest of this paper is organized as follows. Section 2 introduces ITS security architecture and some corresponding cryptographic techniques. Section 3 presents three secret-sharing schemes in detail. Section 4 proposes the threshold key management scheme for ITS security. Section 5 draws the conclusion for this paper.

2. Related Works

Cryptography plays a vital role in protecting the security of ITS. Figure 1 shows the mechanism in protecting ITS security and the corresponding cryptography primitives.

The ITS security architecture mainly includes access management, security management, and data encryption. In particular, access management consists of user authentication and access control. Security management can be classified into decentralize management and centralize management. Data encryption falls into two categories: the encryption at the client side and the encryption at the server side. Generally speaking, the encryption at the server side can achieve higher security level than the encryption at the client side.

On the contrary, various cryptography technologies can be used to protect ITS security. Figure 1 lists some effective and well-designed schemes in cryptography, which can be employed at the different branches of ITS architecture to ensure security. In the access management branch, MAC and digital signature are suitable. Currently, the most commonly used techniques in digital signature are BLS

signature [16], group signature [17], and ring signature [18]. BLS signature has many desirable properties such as the length of the signature, which is short, and the aggregability of the signature. The group signature and ring signature enable a group of users to sign on a message with properties of anonymity, traceability, and unforgeability. In the data encryption branch, various encryption schemes in cryptography can be referred to protect the data security of both the client side and the server side. Generally speaking, the encryption can be divided into the symmetric encryption and the asymmetric encryption. In addition, the key management [19] plays an essential role in both the symmetric encryption and the asymmetric encryption. At present, the well-recognized symmetric encryption schemes are DES, AES, RC6, and TwoFish, while the cutting edge asymmetric encryption schemes include the searchable encryption [20] and homomorphic encryption [21]. The key management is an essential mechanism in encryption, which ensures the security of the key. Improper key management may threaten the security of encrypted data. The key exchange protocol [22], secret sharing [23], and hierarchical key management [24] are effective methods in key management. In this paper, we mainly focus on the secret-sharing scheme to protect ITS security.

The main contributions of this paper can be summarized as follows:

- (1) ITS security architecture is presented. In this paper, the main branches of ITS security are outlined. In addition, the corresponding cryptographic technologies are listed, which can ensure the security of ITS.
- (2) Three kinds of secret-sharing schemes are studied in this paper. The mainstream schemes in the field of secret sharing are being studied. In particular, Shamir's secret-sharing scheme, Blakley's secret-sharing scheme, and CRT secret-sharing scheme are studied in this paper.
- (3) The threshold key management scheme for ITS security is designed. Based on Shamir's secret-sharing scheme and the CRT secret-sharing scheme, we proposed the threshold key management scheme. The proposed scheme enables n stakeholders to share data and gives each stakeholder the control over the data. Note that the fault tolerance is also supported by taking advantage of the secret-sharing scheme. Namely, the system can perform well, provided that, at least, t stakeholders are legal.

In the paper, aiming at the security threats in ITS, the secret-sharing schemes are employed in the blockchain-based ITS to support threshold key management, thus, ensuring the reliability and the privacy of ITS.

3. Secret-Sharing Schemes

In this section, three types of secret sharing are introduced. Generally speaking, a secret sharing in cryptography is a scheme that enables the division of a secret s into n shares such that if and only if the combination of at least t shares

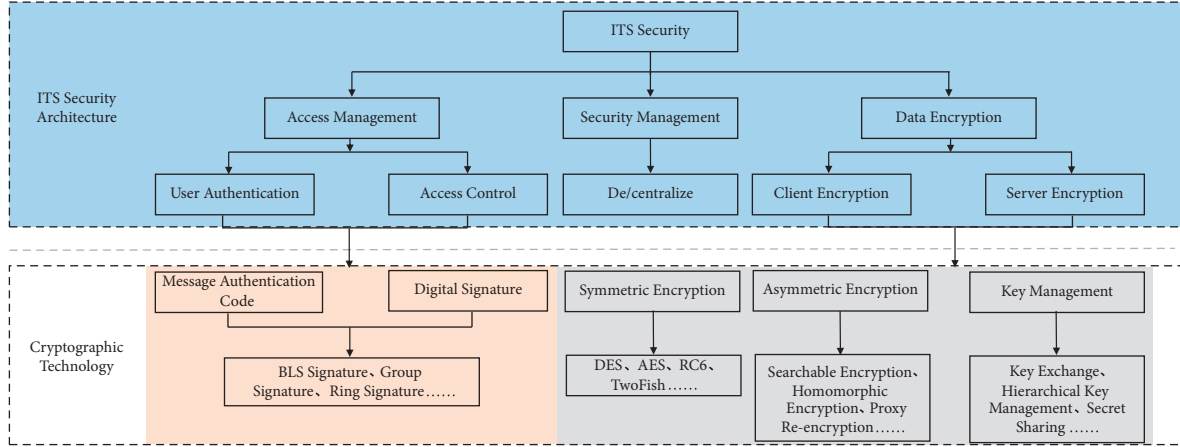


FIGURE 1: ITS security architecture and the corresponding cryptographic technologies.

can recover the secret. The secret sharing with t threshold can also be named (t, n) secret sharing.

3.1. Shamir's Secret Sharing. The secret-sharing scheme [25] proposed by Shamir is based on the Lagrange polynomials. Essentially, the basic idea of Shamir's scheme is based on the fact that two points decide a line, three points decide a parabola, and so on. In general, a polynomial of degree $t - 1$ can be defined by t points on it. Specifically, a polynomial $f(x)$ of degree $t - 1$ is selected for a secret-sharing scheme with t threshold:

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1}. \quad (1)$$

Here, the coefficient of x is selected at random while the secret is encoded as the constant a_0 . The share that is distributed to distinct stakeholders i is a point in $f(x)$ with random selected x_i and corresponding $y_i = f(x_i)$. In order to recover the secret (i.e., a_0), the corporation of at least t stakeholders is required. In particular, these t stakeholders maintain t point in the curve defined by $f(x)$. Based on the Lagrange polynomial shown in equation (2), these t stakeholders can reconstruct the polynomial $f(x)$, and therefore, recovering the secret a_0 ,

$$L(x) = \sum_{j=0}^{t-1} y_j \cdot l_j(x). \quad (2)$$

From Shamir's works, various secret-sharing schemes based on the Lagrange polynomials were proposed, which can be found in [26–28]. Moreover, Shamir's secret sharing is employed in various applications such as the cloud computing [29, 30] and the privacy-preserving environment [31].

3.2. Blakley's Secret Sharing. The secret-sharing scheme [32] proposed by Blakley is based on the hyperplanes. The basic fact of Blakley's secret sharing is that n nonparallel hyperplanes in n -dimensional space must intersect at exactly one

point. For example, three nonparallel planes must intersect at exactly one point in 3-dimensional space. In this scheme, with n stakeholders and t threshold, the secret is encoded as a point in a t -dimensional space, while the share of each stakeholder is the affine hyperplane that passes through the secret point (it is clear that the number of the affine hyperplane is infinite). In particular, the affine hyperplanes in the t -dimensional space can be defined by

$$a_1x_1 + a_2x_2 + a_3x_3 + \dots + a_tx_t = b. \quad (3)$$

In order to generate n share for n stakeholders, t random coefficients are selected for stakeholder i and corresponding y_i can be calculated as

$$y_i = a_1^i x_1 + a_2^i x_2 + a_3^i x_3 + \dots + a_t^i x_t. \quad (4)$$

Note that the secret is encoded as one coordinate x_t , which is fixed and the rest $t - 1$ coordinates can be selected at random. Any t stakeholders together can calculate the secret by solving the solution of

$$\begin{pmatrix} a_1^1 a_2^1 a_3^1 \dots a_t^1 \\ a_1^2 a_2^2 a_3^2 \dots a_t^2 \\ a_1^3 a_2^3 a_3^3 \dots a_t^3 \\ \dots \\ a_1^t a_2^t a_3^t \dots a_t^t \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \dots \\ x_t \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ \dots \\ y_t \end{pmatrix}. \quad (5)$$

Blakley's secret sharing has also been studied and improved since it has been proposed. In [33–35], the extension and application of Blakley's secret sharing can be found.

3.3. CRT Secret Sharing. The secret-sharing scheme [36] proposed by Asmuth and Bloom is based on Chinese remainder theorem (CRT).

Given a set of pairwise co-prime number $m_1, m_2, m_3, \dots, m_n$, the following linear congruence equations have a unique solution for modular M , where $M = \prod_{i=1}^n m_i$:

$$\begin{cases} a_1 \bmod m_1 = x, \\ a_2 \bmod m_1 = x, \\ a_3 \bmod m_1 = x, \\ \dots, \\ a_n \bmod m_1 = x. \end{cases} \quad (6)$$

Moreover, the unique solution can be calculated by

$$x \equiv \left[\sum_{i=1}^n a_i C_i (C_i^{-1} \bmod m_i) \right] \bmod M, \quad (7)$$

where $C_i = M/m_i$.

CRT is a fundamental theorem in cryptography; the CRT-based secret sharing has always been studied since it was proposed. The recent research progress in the CRT-based secret sharing can be found in [37–39].

In the following, we employ these three kinds of secret-sharing schemes to design the threshold key management scheme for multiple stakeholders in ITS.

4. Threshold Key Management for Database Security

In this section, the threshold key management scheme in blockchain-based ITS is proposed based on the secret-sharing scheme.

4.1. The System Model. In this section, the system model of the threshold key management for blockchain-based ITS security is presented. Figure 2 depicts the system model. In the system model, the shared data are possessed by n vehicles. In order to facilitate the use and sharing [40], they want to store the data in the cloud. However, storing plaintext data may bring many security issues. Thus, these n vehicles can generate a key to encrypt data to ensure data storage security. In our system, the secret-sharing scheme is utilized to generate the key. Note that, in the secret-sharing scheme, the key is divided into n pieces and distributed to n vehicles in a secure channel. After that, if and only if at least t vehicles together can recover the key, here, t is the threshold of the secret-sharing scheme. In this way, the data are protected with the following properties:

- (i) Each of the n vehicles has control over the data. Specifically, any t vehicles of these n vehicles together can recover the key. Thus, they can decrypt the data.
- (ii) The invalidation of some vehicles will not cause the key to be unrecoverable. More precise, the invalidation of $n - t + 1$ is tolerable.

4.2. Cross-Domain Communication Architecture. The architecture of ITS cross-domain communication changes when the blockchain technology is introduced. Figure 3 shows the cross-domain communication in ITS of the traditional architecture. In Figure 3, it can be observed that the communication between vehicles in distinct domains triggers five channels including the communication between

vehicle and RSU, the communication between CA and RSU, and the communication between CAs. The detailed channels are marked with red color in Figure 3. In contrast, Figure 4 shows the cross-domain communication in ITS of the blockchain-based architecture. It can be seen in Figure 4 that the communication of vehicles in distinct domains can be simplified by the blockchain network. Also, by taking advantage of the blockchain technology, the reliability of the communication can be guaranteed.

4.3. Key Management Scheme Based on Shamir's Secret Sharing. Based on Shamir's secret sharing, the key management scheme for blockchain-based ITS can be designed as follows:

- (i) Key generation: to share data D for n stakeholders, the owner of the data D selected a random AES key. The key can be $\text{key} \leftarrow \{0, 1\}^l$. Here, l is the security parameter of the system, which can be 128-bit, 192-bit, or 256-bit depending on the security level of the system.
- (ii) Threshold selection: the n stakeholders jointly decide the threshold t .
- (iii) Polynomial generation: the owner of the data selects a polynomial of degree $t - 1$ as equation (1). The key is encoded as the constant a_0 , while the other $t - 1$ coefficients are selected randomly.
- (iv) Share generation: for each stakeholder i , the data owner chooses a point x_i and calculates the corresponding y_i . Then, the data owner distributes the pair (x_i, y_i) to stakeholder i . To distribute key for n stakeholders, the data owner needs to calculate n pairs of (x_i, y_i) and distribute these pairs to the corresponding stakeholder in a secure way.
- (v) Encryption: after the key distribution, the data owner encrypts data D with key and uploads the encrypted data E to the cloud. Here, $E = \text{AES}_{\text{key}}(D)$.
- (vi) Decryption: with the received part, a stakeholder, together with other $t - 1$ stakeholders, can recover the key. After that, these stakeholders can decrypt the encrypted data E .

In the following, an example is presented for the key management scheme. In this example, 10 stakeholders are involved and the threshold is 4. The selected polynomial is shown equation (8). The corresponding secret is 2006, which is in a decimal form:

$$f(x) = 2006 + 8x + 25x^2 + 30x^3. \quad (8)$$

The 10 pairs of (x_i, y_i) are distributed to each stakeholders. Table 1 shows the 10 pairs of (x_i, y_i) selected based on equation (7). Here, in order to facilitate readers' understanding, x is set from 2 to 11. We note that, in practice, the value of x_i can be selected randomly over the function domain to preserve security.

Then, we show that any 4 pairs from Table 1 can be used to recover the secret 2006. In the example, (4, 4358),

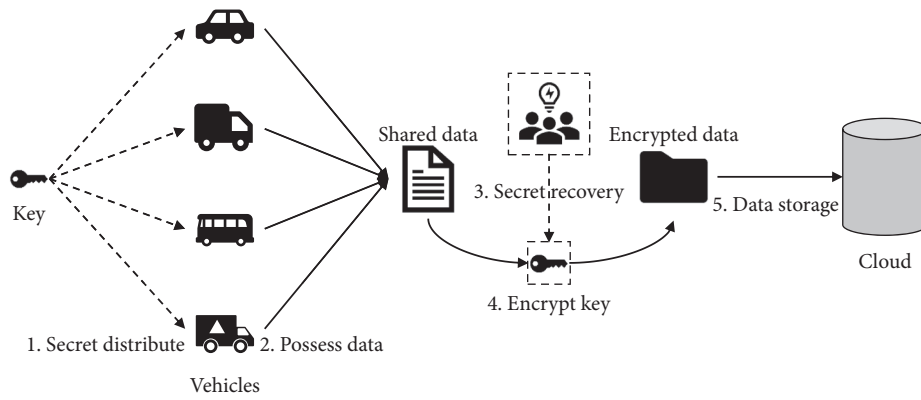


FIGURE 2: The system model.

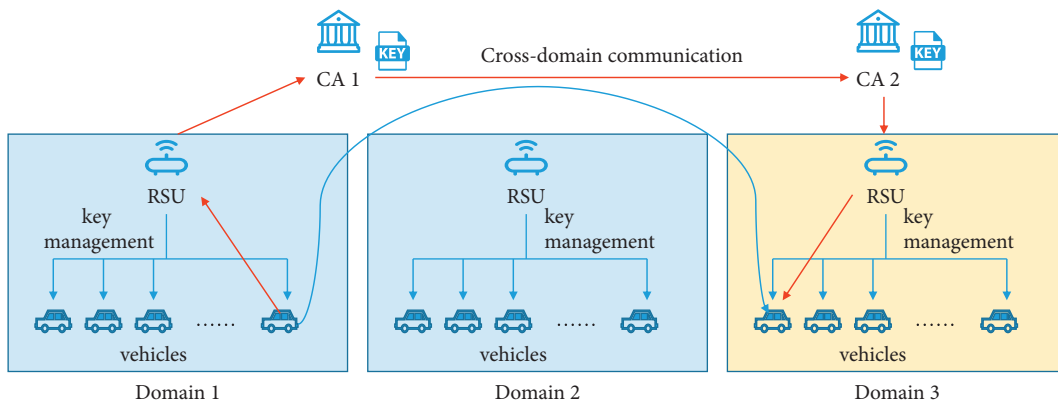


FIGURE 3: The traditional cross-domain communication architecture.

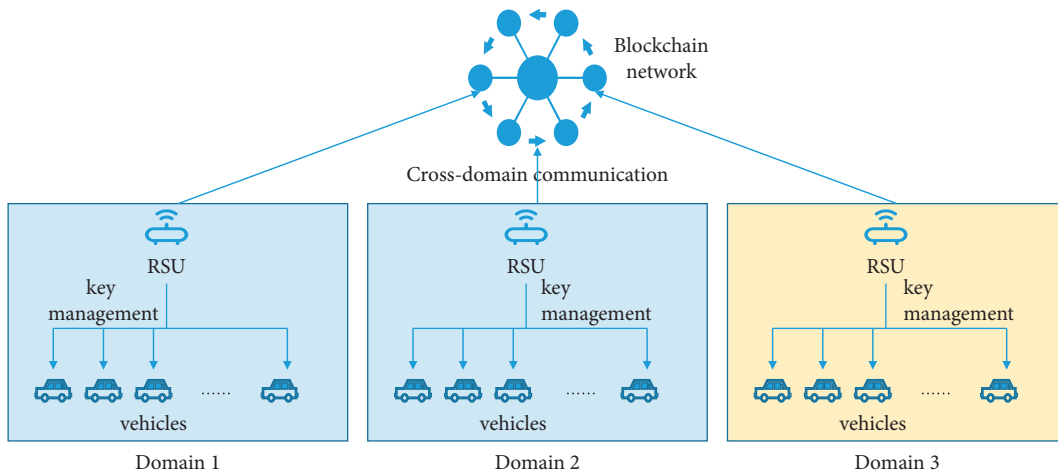


FIGURE 4: The blockchain-based cross-domain communication architecture.

TABLE 1: The distributed for 10 stakeholders.

x	2	3	4	5	6	7	8	9	10	11
y	2362	3065	4358	6421	9493	13577	19030	25973	34586	45049

(5, 6421), (6, 9493), and (7, 13577) are selected for the secret recovery. In equation (2), $l_j(x)$ is Lagrange basis polynomials, which is shown in equation (8):

$$l_j(x) = \sum_{i=0, i \neq j}^t \frac{x - x_i}{x_j - x_i}. \quad (9)$$

$$\begin{aligned} L(x) &= \sum_{j=0}^{t-1} y_j \cdot l_j(x) \Rightarrow L(0) = \sum_{j=0}^{t-1} y_j \cdot l_j(x) \\ &= y_1 \cdot \sum_{i=1, i \neq 1}^4 \frac{-x_i}{x_1 - x_i} + y_2 \cdot \sum_{i=1, i \neq 2}^4 \frac{-x_i}{x_2 - x_i} + y_3 \cdot \sum_{i=1, i \neq 3}^4 \frac{-x_i}{x_3 - x_i} + y_4 \cdot \sum_{i=1, i \neq 4}^4 \frac{-x_i}{x_4 - x_i} \\ &= 4358 \cdot \frac{5}{5-4} \cdot \frac{6}{6-4} \cdot \frac{7}{7-4} + 6421 \cdot \frac{4}{4-5} \cdot \frac{6}{6-5} \cdot \frac{7}{7-5} + 9434 \cdot \frac{4}{4-6} \cdot \frac{5}{5-6} \cdot \frac{7}{7-6} + 13577 \cdot \frac{4}{4-7} \cdot \frac{5}{5-7} \cdot \frac{6}{6-7} \\ &= 4358 \cdot 35 - 6421 \cdot 84 + 9434 \cdot 70 - 13577 \cdot 20 \\ &= 2006. \end{aligned} \quad (10)$$

It can be observed from equation (9) that the secret value 2006 is recovered by 4 pairs (x_j, y_j) of the polynomial. In fact, any 4 pairs are sufficient for the secret recovery based on the interpolation polynomial.

In addition, Figure 5 depicts three different polynomials constructed based on the selected secret 2006. In Figure 5, the polynomial of y_1 , y_2 , and y_3 are $y_1 = 2006 + 10x + 45x^2 + 56x^3$, $y_2 = 2006 + 25x + 60x^2 + 80x^3$, and $y_3 = 2006 + 8x + 25x^2 + 30x^3$, respectively.

4.4. Key Management Scheme Based on CRT. Based on CRT secret sharing, the key management scheme for blockchain-based ITS can be designed as follows:

- (i) Key generation: this phase is identical to the key management scheme based on Shamir's secret sharing. The data owner selects an AES key.
- (ii) Threshold selection: the n stakeholders jointly decide the threshold t .
- (iii) Parameters' selection: the owner of the data selects n co-prime numbers m such that $(m_i, m_j) = 1$ holds for each pair of m_i and m_j , ($i \neq j$). After that, based on the selected threshold, the owner of the data calculates the product of these n co-prime numbers as $M = \sum_{i=1}^t m_i$. Here, the selected key should satisfy $0 \leq \text{key} < m_1$.
- (iv) Share generation: to divide the secret key, the data owner selects a random number r and calculates

Note that based on equations (2) and (9) and the four selected pairs, the secret can be recovered. Equation (10) shows the calculation in detail:

$S = \text{key} + r \cdot m_1$. Here, the selected random number r should satisfy $0 \leq r < M/m_1 - 1$.

- (v) Share distribution: for each stakeholder i ($i > 1$), the data owner distributes S_i to stakeholder i . Here, $S_i = S \bmod m_i$. Similarly, this value is transmitted in a secure way.
- (vi) Encryption and decryption: after the key distribution, the data owner encrypts data D with key and uploads the encrypted data E to the cloud. In addition, the decryption needs the involvement of at least t stakeholders. They can construct the following linear congruence equations:

$$\begin{cases} S_2 \bmod m_2 = S, \\ S_3 \bmod m_3 = S, \\ S_4 \bmod m_4 = S, \\ \dots, \\ S_t \bmod m_t = S. \end{cases} \quad (11)$$

Based on CRT, this linear congruence equations has a unique solution:

$$S = \sum_{i=2}^t S_i \cdot C_i \cdot (C_i^{-1} \bmod m_i) \bmod M^*, \quad (12)$$

where $M^* = \prod_{i=2}^t m_i$ and $C_i = M^*/m_i$.

To show the performance of CRT and Shamir's secret-sharing-based key management scheme, the complexity of

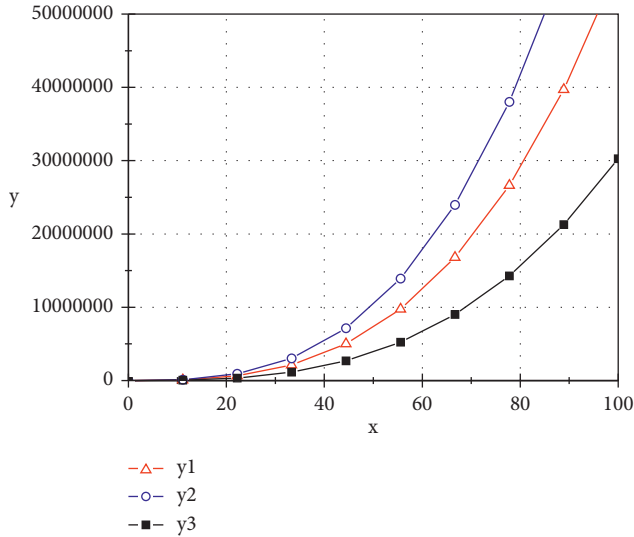


FIGURE 5: The different polynomials of the same selected secret.

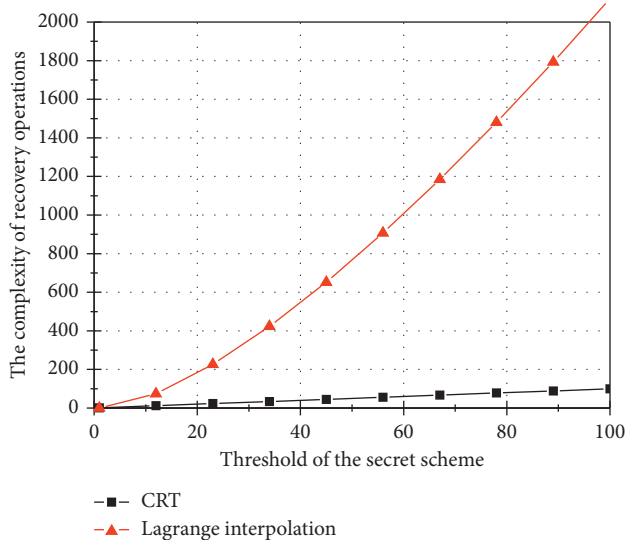


FIGURE 6: The comparison between Shamir's secret sharing and CRT secret sharing.

recovery operations of these two schemes is analyzed. Figure 6 depicts the comparison between Shamir's secret-sharing-based key management scheme and CRT secret-sharing-based key management scheme. It can be observed from Figure 6 that the scheme based on CRT is more efficient than the scheme based on Shamir's secret sharing.

5. Conclusion

In this paper, blockchain-based ITS architecture and the corresponding cryptographic technologies are presented. Moreover, the threshold key management scheme for blockchain-based ITS is proposed. To achieve threshold key management, the secret-sharing schemes are employed, which supports threshold key sharing for multiple

stakeholders. Taking advantage of the secret-sharing schemes, the security and fault tolerance data sharing in ITS can be supported. The comparison of CRT and Shamir's secret sharing-based key management scheme is also conducted, which indicates that CRT-based scheme has an advantage over Shamir's secret-sharing-based scheme on the complexity of recovery operations.

Data Availability

The performance data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (U1836115, 61672295, 61922045, and 61672290), the Peng Cheng Laboratory Project of Guangdong Province (PCL2018KP004), the Postgraduate Research & Practice Innovation Program of Jiangsu Province (KYCX21_0998 and KYCX21_1003), the CICAET fund, and the PAPD fund.

References

- [1] J. Shen, T. Zhou, J. Lai, P. Li, and S. Moh, "Secure and efficient data sharing in dynamic vehicular networks," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8208–8217, 2020.
- [2] Y.-S. Su, T.-J. Ding, and M.-Y. Chen, "Deep learning methods in internet of medical things for valvular heart disease screening system," *IEEE Internet of Things Journal*, p. 1, 2021.
- [3] J. Liang, Z. Qin, S. Xiao, L. Ou, and L. Lin, "Efficient and secure decision Tree classification for cloud-assisted online diagnosis services," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 4, pp. 1632–1644, 2021.
- [4] J. Zhang, F.-Y. Wang, K. Wang, W.-H. Lin, X. Xu, and C. Chen, "Data-driven intelligent transportation systems: a survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 4, pp. 1624–1639, 2011.
- [5] H. Tan and I. Chung, "Rsu-aided remote v2v message dissemination employing secure group association for uav-assisted vanets," *Electronics*, vol. 10, no. 5, p. 548, 2021.
- [6] Y.-X. Zhao, Y.-S. Su, and Y.-C. Chang, "A real-time bicycle record system of ground conditions based on internet of things," *IEEE Access*, vol. 5, pp. 17525–17533, 2017.
- [7] C. Wang, R. Huang, J. Shen, J. Liu, P. Vijayakumar, and N. Kumar, "A novel lightweight authentication protocol for emergency vehicle avoidance in VANETs," *IEEE Internet of Things Journal*, 2021.
- [8] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.
- [9] H. Tan, P. Kim, and I. Chung, "Practical homomorphic authentication in cloud-assisted vanets with blockchain-based healthcare monitoring for pandemic control," *Electronics*, vol. 9, no. 10, p. 1683, 2020.
- [10] C. E. Shannon, "A mathematical theory of secrecy systems," *Bell system technical Journal*, vol. 28, pp. 623–656, 1949.

- [11] A. Setyono and D. Rosal Ignatius Moses Setiadi, "Stegocrypt method using wavelet transform and one-time pad for secret image delivery," in *Proceedings of the 2017 4th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*, pp. 203–207, IEEE, Semarang, Indonesia, October 2017.
- [12] G. Scerri and R. Stanley-Oakes, "Analysis of key wrapping apis: generic policies, computational security," in *Proceedings of the 2016 IEEE 29th Computer Security Foundations Symposium (CSF)*, pp. 281–295, IEEE, Lisboa, Portugal, July 2016.
- [13] T. Zhou, J. Shen, X. Li, C. Wang, and H. Tan, "Logarithmic encryption scheme for cyber-physical systems employing Fibonacci Q-matrix," *Future Generation Computer Systems*, vol. 108, pp. 1307–1313, 2020.
- [14] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.
- [15] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
- [16] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, pp. 514–532, Springer, Singapore, December 2021.
- [17] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," in *Proceedings of the Annual International Cryptology Conference*, pp. 410–424, Springer, Santa Barbara, CA, USA, August 2020.
- [18] S.-F. Sun, M. H. Au, J. K. Liu, and T. H. Yuen, "Ringct 2.0: a compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero," in *Proceedings of the European Symposium on Research in Computer Security*, pp. 456–474, Springer, Guildford, England, September 2020.
- [19] T. Zhou, H. Yang, and J. Shen, "Key agreement protocol with dynamic property for vanets," *Journal of Cryptologic Research*, vol. 7, no. 3, pp. 1–14, 2020.
- [20] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Future Generation Computer Systems*, vol. 95, pp. 420–429, 2019.
- [21] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes," *ACM Computing Surveys*, vol. 51, no. 4, pp. 1–35, 2018.
- [22] A. Faz-Hernández, J. López, E. Ochoa-Jiménez, and F. Rodríguez-Henríquez, "A faster software implementation of the supersingular isogeny Diffie-Hellman key exchange protocol," *IEEE Transactions on Computers*, vol. 67, pp. 1622–1636, 2017.
- [23] J. Shen, T. Zhou, X. Liu, and Y.-C. Chang, "A novel Latin-square-based secret sharing for m2m communications," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3659–3668, 2018.
- [24] A. Albakri, L. Harn, and S. Song, "Hierarchical key management scheme with probabilistic security in a wireless sensor network (WSN)," *Security and Communication Networks*, vol. 2019, Article ID 3950129, 11 pages, 2019.
- [25] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
- [26] E. Dawson and D. Donovan, "The breadth of Shamir's secret-sharing scheme," *Computers & Security*, vol. 13, no. 1, pp. 69–78, 1994.
- [27] K. Benzekki, A. El Fergougui, and A. E. Elalaoui, "A verifiable secret sharing approach for secure multicloud storage," in *Proceedings of the International Symposium on Ubiquitous Networking*, pp. 225–234, Springer, Limoges, France, May 2019.
- [28] J. K. Arbogast, I. B. Sumner, and M. O. Lam, "Parallelizing shamir's secret sharing algorithm," *Journal of Computing Sciences in Colleges*, vol. 33, pp. 12–18, 2018.
- [29] S. N. Pundkar and N. Shekhar, "Cloud computing security in multi-clouds using shamir's secret sharing scheme," in *Proceedings of the 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, pp. 392–395, IEEE, Chennai, India, March 2016.
- [30] T. Zhou, L. Chen, and J. Shen, "Movie recommendation system employing the user-based cf in cloud computing," in *Proceedings of the IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, pp. 46–50, IEEE, Guangzhou, China, July 2017.
- [31] Q. Li and M. G. Christensen, "A privacy-preserving asynchronous averaging algorithm based on shamir's secret sharing," in *Proceedings of the 2019 27th European Signal Processing Conference (EUSIPCO)*, pp. 1–5, IEEE, A Coruña, Spain, September 2019.
- [32] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the 1979 International Workshop on Managing Requirements Knowledge (MARK)*, pp. 313–318, IEEE, New York, NY, USA, June 1979.
- [33] G. Blakley and G. Kabatianskii, "Linear algebra approach to secret sharing schemes," in *Workshop on Information Protection*, pp. 33–40, Springer, Berlin, Heidelberg, 1993.
- [34] I. N. Bozkurt, K. Kaya, A. A. Selçuk, and A. M. Güloğlu, "Threshold cryptography based on Blakely secret sharing," in *Proceedings of the Information Security and Cryptology*, pp. 313–317, Ankara, Turkey, 2008.
- [35] Z. Xia, B. Yang, Y. Zhou, M. Zhang, and Y. Mu, "Improvement of attribute-based encryption using Blakely secret sharing," in *Proceedings of the Australasian Conference on Information Security and Privacy*, pp. 631–641, Springer, Perth, Australia, December 2019.
- [36] C. Asmuth and J. Bloom, "A modular approach to key safeguarding," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 208–210, 1983.
- [37] O. Ersoy, T. B. Pedersen, and E. Anarim, "Homomorphic extensions of CRT-based secret sharing," *Discrete Applied Mathematics*, vol. 285, pp. 317–329, 2020.
- [38] X. Jia, D. Wang, D. Nie, X. Luo, and J. Z. Sun, "A new threshold changeable secret sharing scheme based on the Chinese remainder theorem," *Information Sciences*, vol. 473, pp. 13–30, 2019.
- [39] O. Ersoy, T. B. Pedersen, K. Kaya, A. A. Selçuk, and E. Anarim, "A CRT-based verifiable secret sharing scheme secure against unbounded adversaries," *Security and Communication Networks*, vol. 9, no. 17, pp. 4416–4427, 2016.
- [40] J. Shen, H. Yang, P. Vijayakumar, and N. Kumar, "A privacy-preserving and untraceable group data sharing scheme in cloud computing," *IEEE Transactions on Dependable and Secure Computing*, 2021.