Hindawi
Security and Communication Networks
Volume 2021, Article ID 1864514, 8 pages
https://doi.org/10.1155/2021/1864514

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]

[1]*School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing, China*
[2]*Cyberspace Security Research Center, Peng Cheng Laboratory, Shenzhen, China*
[3]*Suqian 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

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 unpractical 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 aggregatability 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

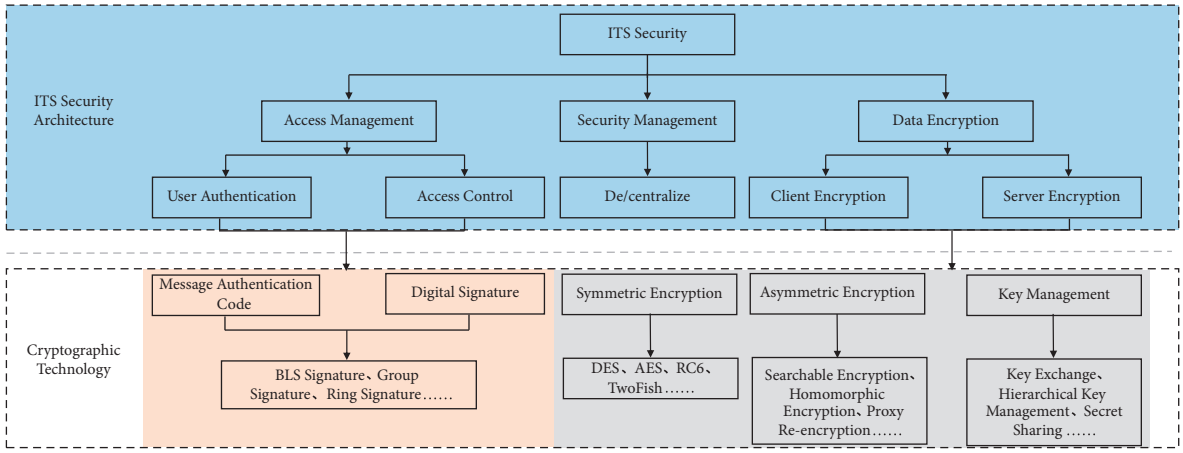

Figure 1: ITS security architecture and the corresponding cryptographic technologies.

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:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}. \tag{1}$$

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,

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

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 stakeholders 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

$$a_1 x_1 + a_2 x_2 + a_3 x_3 + \cdots + a_t x_t = b. \tag{3}$$

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

$$y_i = a_1^i x_1 + a_2^i x_2 + a_3^i x_3 + \cdots + a_t^i x_t. \tag{4}$$

Note that the secret is encoded as one coordinate x_i, 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

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

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 $m_1, m_2, m_3, \ldots, m_n$, the following linear congruence equations have a unique solution for modular M, where $M = \prod_{i=1}^{n} m_i$:

$$\begin{cases} a_1 \bmod m_1 = x, \\ a_2 \bmod m_1 = x, \\ a_3 \bmod m_1 = x, \\ \ldots, \\ a_n \bmod m_1 = x. \end{cases} \tag{6}$$

Moreover, the unique solution can be calculated by

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

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 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, $E = AES_{\text{key}}(D)$.

(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:

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

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),

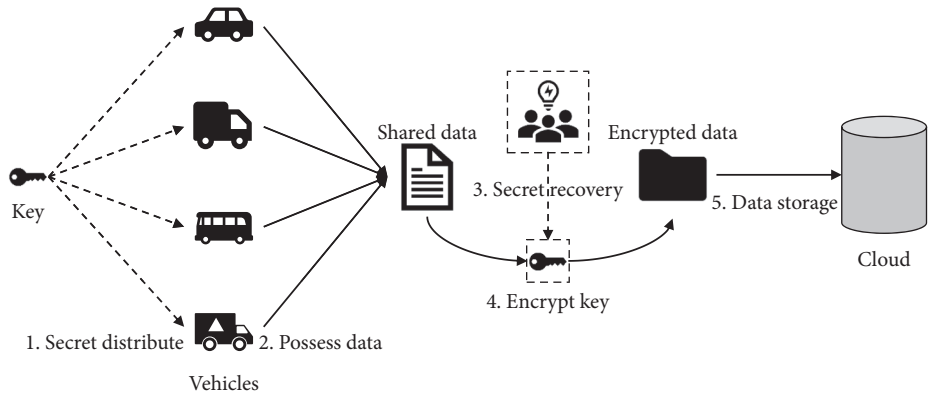

Figure 2: The system model.

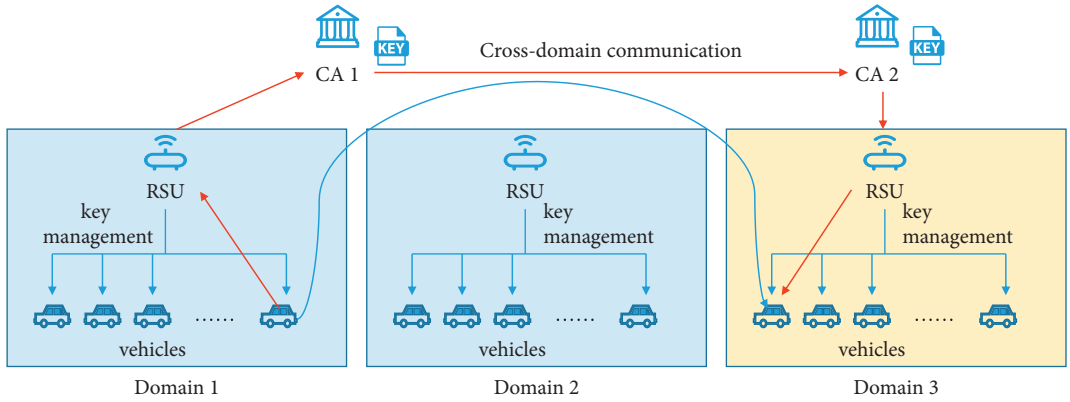

Figure 3: The traditional cross-domain communication architecture.

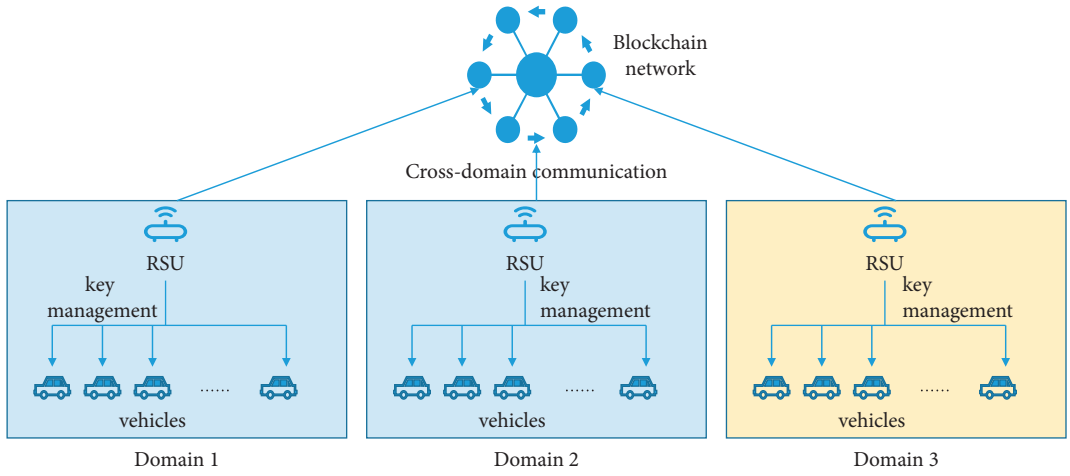

Figure 4: The blockchain-based cross-domain communication architecture.

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):

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

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:

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

It can be observed from equation (9) that the secret value 2006 is recovered by 4 pairs (x_i, y_i) 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 $M = \prod_{i=1}^{t} m_i$. 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 $S = \text{key} + r \cdot m_1$. 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:

$$\begin{cases} S_2 \bmod m_2 = S, \\ S_3 \bmod m_3 = S, \\ S_4 \bmod m_4 = S, \\ \cdots\cdots, \\ S_t \bmod m_t = S. \end{cases} \tag{11}$$

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

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

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

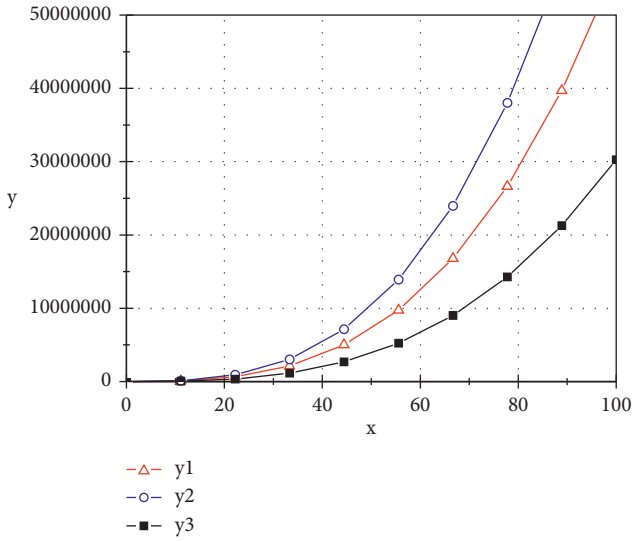

Figure 5: The different polynomials of the same selected secret.

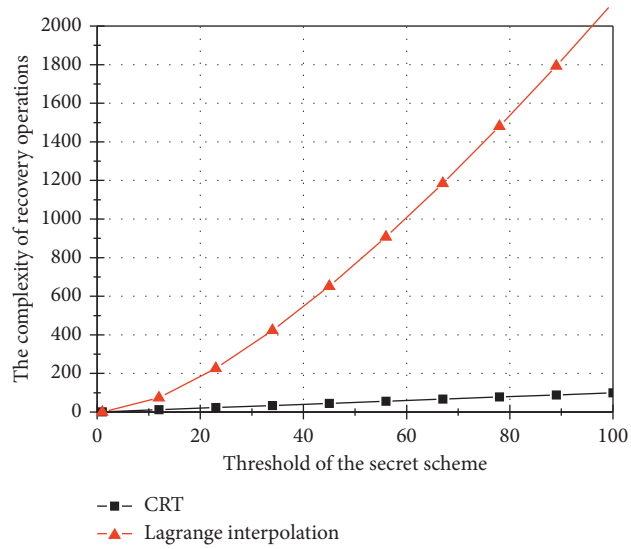

Figure 6: The comparison between Shamir's secret sharing and CRT secret sharing.

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 CICAEET 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 *Proceedins 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. Shekokar, "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. Selcuk, and A. M. Güloglu, "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 Blakley 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.