Hindawi
Security and Communication Networks
Volume 2022, Article ID 5424395, 8 pages
https://doi.org/10.1155/2022/5424395

Research Article

A Decentralized Electronic Reporting Scheme with Privacy Protection Based on Proxy Signature and Blockchain

Huiying Zou,[1,2] Xiaofan Liu,[2] Wei Ren,[1,2,3] and Tianqing Zhu[2]

[1]*State Key Laboratory of Public Big Data, Guizhou University, Guiyang 550025, China*
[2]*School of Computer Science, China University of Geosciences, Wuhan, China*
[3]*Yunnan Key Laboratory of Blockchain Application Technology, Kunming, China*

Correspondence should be addressed to Wei Ren; weirencs@cug.edu.cn

Received 19 October 2021; Revised 6 January 2022; Accepted 8 January 2022; Published 7 February 2022

Academic Editor: Mamoun Alazab

The electronic reporting system can alleviate the problems in terms of efficiency, content confidentiality, and reporter privacy imposed in the traditional reporting system. Relying on anonymity, the privacy of reporters can be protected, but the authentication of reporters with fake names should also be maintained. If authenticated anonymity is guaranteed, the reporters may still conduct misbehaviors such as submitting fake reports after the authentication. To address the above dilemma, we propose to apply a proxy signature to achieve authenticated anonymity and employ blockchain to maintain anonymity yet guarantee traceability for reporters' misbehaviors. We also propose a new proxy signature scheme in this paper by module lattice for postquantum security. The extensive analysis justified our proposed scheme is secure and manageable.

1. Introduction

Unlike the traditional offline reporting method, where reporting letter is written by a reporter and sent to the relevant department, the electronic reporting system is more convenient and efficient. Anyone can report some content about anyone to a special department at any time anywhere. However, electronic reporting usually meets with some security problems as follows: to protect the identity of reporters, reporters usually must be anonymous. A dilemma thus arises in how to authenticate the reporter whose names are fake; if they can be authenticated in a fake name, also called authenticated anonymity, they may further report fake information. Hence, traceability should also be guaranteed.

We observe that current research have not extensively addressed the above dilemma. Or only solve one-half of the problem, either (authenticated) anonymity or traceability. In this paper, we try to solve both "birds" together with one stone. More specifically, we apply a proxy signature to achieve authenticated anonymity and we employ blockchain to obtain traceability.

Proxy signature is a kind of advanced digital signature, to which the proxy signer is delegated to generate the signature on behalf of the original signer. The reporter can send his message to a reputable third party to check, and the third-party delegate to generate the signature based on his own report message.

Blockchain presents the properties of immutability, distribution, and nonrepudiation. The reporter is a node of the blockchain, which only communicates with the trusted third party. If a malicious node wants to forge a reporting message, it is easy to find out by blockchain. According to the properties of proxy signature and blockchain, we can use them to guarantee that every reporter is honest and the reporting message is credible.

In this paper, we design this electronic reporting scheme with privacy protection based on proxy signature and blockchain. The contributions of this paper are as follows:

(i) We apply proxy signature and blockchain technology for building a decentralized electronic reporting scheme. At the same time, our proposed scheme can achieve auditable yet authenticated anonymity, that is, preserve the reporter's privacy, authenticate

anonymous reporters upon reporting, and trace misbehaviors of anonymous reporters.

(ii) We propose a new postquantum proxy signature based on the module lattice and provide the complete correctness analysis.

The rest of the paper is organized as follows: Related and required background information is briefly introduced in Section 2 and Section 3. In Section 4, we describe both the system models and the adversary models. We illustrate our proposed scheme in Section 5 and evaluate its security and efficiency in Section 6. Finally, we conclude this paper in Section 7.

2. Related Works

In 1996, Mambo, Usuda, and Okamoto [1, 2] proposed the idea and algorithm of proxy signature in the ACM CCS96 conference. Proxy signatures are now widely used in blockchain technology. Wang et al. [3] proposed a proxy signature mechanism based on the ElGamal algorithm in order to address the problem that the signature power of nodes cannot be transferred to blockchains, which is suitable for the management model of Sharing energy storage (SES) on blockchains. Shen et al. [4] proposed a lightweight threshold certificate authority framework LTCA by devising a threshold proxy signature, where the proxy signing key is issued by a coalition of a threshold number of certificate authorities (CAs) playing the roles of authorized nodes in the consortium blockchain. Then based on the proposed LTCA, an efficient privacy-preserving location-based service protocol (PPVC) is contrived to protect each vehicle's conditional identity privacy with a moderate cost. Pawlak et al. [5], based on the multiproxy signature technology, used the idea of a multi-intelligence system and intelligent agents and proposed a blockchain-based Internet voting system with end-to-end verifiable and auditable implementation. On the one hand, many other theoretical schemes about the proxy signature have been proposed [6–8]. On the other hand, blockchain, as a novel distributed consensus scheme, also plays a great role in various fields [9–12]. Besides, there are also other similar works [14, 15, 26, 28, 29].

In recent years, e-government has been stepping into the relationship between the government and citizens in many countries [16, 17]. It has become a powerful assistant for the government to serve the people. Among them, e-reporting has beaten traditional reporting with absolute advantages of convenience and security and has become the main way for citizens to exercise their reporting rights. The research on electronic reporting is constantly updated and improved with the development of the Internet. Wang et al. [18] first proposed the concept of a blockchain-based anonymous reporting mechanism (BB2AR), and on this basis, they proposed and implemented a BB2AR scheme based on elliptic curve public key cryptosystem. Adeshina and Ojo [19] proposed a new secure reporting system based on bit commitment. The scheme keeps the reporter's privacy in an ordinary routine, but the anonymity can be removed by a trusted thirty party (TTP) with the cooperation from the electronic reporting center (EIC). Wang et al. [20] have come up with ReportCoin, a blockchain-based incentive anonymous reporting system that ensures the confidentiality of user identities and the reliability of reporting messages. Most of the existing electronic reporting schemes use group signature or ring signature, which are designed with the anonymity of the reporter as the necessary requirement. The related works are illustrated in Table 1.

To sum up, we combined several advantages of existing research work and designed a new electronic reporting scheme to meet the requirements of unforgeability and immutability.

3. Preliminaries

3.1. Proxy Signature. Proxy signature was first proposed by Mambo, Usuda, and Okamoto [12] in 1996. Proxy signature is a special signature scheme, in which the original signer grants his signature right to the proxy signer, and the proxy signer can generate a valid digital signature on behalf of the original signature. A proxy signature algorithm usually has the following five steps:

(1) Initialization: generating the key and other parameters required for proxy signature according to the algorithm.

(2) Parameter transfer: the original signer calculates the parameters that the proxy signer requires for signing and secretly transmits them to the proxy signer.

(3) Verification of signing right: the proxy signer verifies the parameters he received. If the verification is successful, the signing process can start. If the verification fails, the original signer can be required to perform the first two steps again or the proxy singer can terminate the signing process.

(4) Proxy signature: the proxy signer uses his or her signing power to generate a valid proxy signature for the message.

(5) Signature verification: the party receiving the message verifies if the proxy signature is valid.

3.2. Lattice. Lattice cryptosystem is an antiquantum computing cryptosystem based on NP-hard problems. Lattice theory was initially used in cryptanalysis until Ajtai first proved the difficulty of lattice problems [21] and proposed lattice cryptography with Dwork [22].

Our scheme's security is based on the hardness of the module version of the Short Integer Solution (MSIS) and Learning With Errors problem (MLWE). The distribution of MLWE is randomly distributed a pair (a_i, b_i) from $R_q^l \times R_q$. a_i is chosen uniformly from R_q^l, and $b_i = a_i^T s + e_i$ where $e_i \longleftarrow S_\eta$ and $s \longleftarrow R_q$. The MLWE is commanded to recover s, while giving lots of samples from the MLWE distribution. It is stated that recovering s is impossible, though given $A \longleftarrow R_q^{k\times l}$ and $b = As + e$ where $k = poly(1^\lambda)$, where λ is a secure parameter. The MSIS problem is that given β and $A \longleftarrow R_q^{h\times l}$ where $h = poly(1^\lambda)$, to find a short nonzero preimage x in the lattice which satisfies $Ax = 0$ and $x \le \beta$.

Table 1: The relevant related work.

Related paper	Use blockchain or not	Signature type
[3]	No	Proxy signature
[4]	Yes	Threshold signature
[5]	Yes	Multi-proxy signature
[16]	Yes	Ring signature
[17]	Yes	No signature
[19]	No	No signature
[20]	Yes	Ring signature

However, it is also impossible to find an efficient preimage x in polynomial time.

3.3. Blockchain. Blockchain development began between 2007 and 2009. It is the underlying technology of Bitcoin, known as the "public ledger for storing cryptocurrencies." In fact, although blockchain appeared with Bitcoin, its development not only enhances the value of Bitcoin but also occupies a place for itself in the Internet field. Blockchain has many significant advantages:

Distributed storage: blockchain enables credit-based peer-to-peer transactions in distributed systems where nodes do not need to trust each other.

Immutable: the attacker's control of a single node cannot affect the block data of other nodes and the entire network, and the cost of a successful attack is very high.

Openness: any data content and operation behavior of blockchain are publicly accessible to all nodes in the network.

4. Problem Formulation

4.1. Problem Statement. Reporting is one of the important ways for citizens to participate in politics, and it is also an important way to protect social fairness and civil rights. However, the traditional reporting way is not secure and secret for the reporter since the privacy of the reporter is easy to be exposed by going to the prosecution center or writing a reporting letter. Thus, anonymous reporting is a good way to protect reporters. It would be complicated and inconvenient if the reporting message is false since anyone can easily report without exposing their identity. To deal with this kind of reporting clutter, we can use the blockchain.

Blockchain provides the platform for everyone to join in politics with an equal chance. Users in blockchain can use the assumed name to report the bad people since blockchain has the property of anonymity. To reduce the above kind of reporting clutter, we design a reporting system using the proxy signature based on the blockchain. We randomly predetermined several proxy signers. Only the message signed from them can be verified and then be trusted by the prosecution center. Besides, considering the continuous development of quantum technology, we design a module-lattice-based proxy signature for our reporting system.

4.2. System Model. Our reporting scheme is deployed in the blockchain system. Users in the blockchain play 4 roles: reporter, proxy signer, electronic reporting box, and reporting center.

Reporting center is one special node in the blockchain system and is the trusted third party. Reporting center is voted by all users in the blockchain using the Raft algorithm [27] (Raft is a consensus algorithm for managing a replicated log). Reporting center records the reporter's reporting signature and her/his own privacy in case of the malicious user interferes with the normal operation of the reporting system. When the user provides false reporting information, she/he will be found out by reporting center according to the ever records, and reporting center will broadcast her/his identity and remove her/him. Besides, reporting center also masters the right of permitting the electronic reporting box to verify the signature.

The electronic reporting box is predetermined by reporting center, and one reporting system only has one reporting box. The reporting box collects the reporting signatures and verifies their validity. When one user in this blockchain is reported more than half of the ordinary users (ordinary users do not contain the nodes of reporting box, reporting center, and proxy signer), the reporting box will broadcast her/his crime and remove her/him from the blockchain.

Proxy signer is the blockchain's user whose reporting box and reporting center both trust. A complete reporting system usually has more than one proxy signer, but to explain the process of our scheme for convenience, we suppose only one proxy signer in this system. The proxy signer first authenticates the reporter's identity and then signs for the reporting message if authentication passes.

The reporter can be any of the rest users in the blockchain and can report anyone she/he thinks is a bad guy. The reporter communicates with the proxy signer and authentic herself/himself, and after receiving the proxy signature from the proxy signer, she/he should submit her/his privacy and signature to the reporting center.

The overall structure is illustrated in Figure 1.

4.3. Adversary Model. For the traditional reporting system, the following risks often exist:

(1) Suppose that an adversary $\mathcal{A}$ attacks the system, which could lead to the loss of the reporter's privacy

(2) The proxy signature may not be the reporter's real proxy signature

(3) Suppose that a malicious user $\mathcal{U}$ who reports good people, i.e., submits a false reporting message to the proxy signer

However, our proposed scheme can avoid these risks perfectly, and we will give a detailed security analysis in Section 6.

5. Proposed Scheme

5.1. Overview. Our scheme contains four parts: system initialization, proxy reporting procedure, reporting recording, and verification.

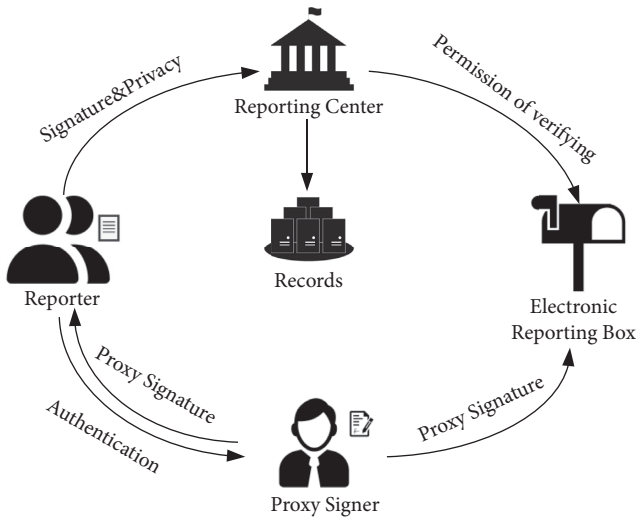

Figure 1: Our reporting system.

For the first step, system initialization, by taking secure parameters as input, users in this system obtain their own public keys and secret keys. In the proxy reporting procedure, a reporter from these members first selects a generally trusted proxy signer and communicates with her/him. Then, the proxy signer completes the authentication of the reporter and generates the proxy signature. The proxy signer sends the proxy signature to the electronic reporting box and the reporter afterward. After receiving the signature, the reporter encrypts her/his privacy (secret key and real name) and signature by the public key of a trusted third party, reporting center, and sends the ciphertext with the time stamp to this trusted third party as the record. The electronic reporting box records the current time after receiving the signature from the proxy signer and verifies whether this signature is valid or not. If the signature is valid, the reporting message will be recorded.

The above participants, including the reporter, the proxy signer, the electronic box, and reporting center, are all in the blockchain system such that our scheme can resist various adversary attacks. With the trusted third party participating, our scheme can trace the attacks from the malicious users while protecting the reporter's privacy (reporter is allowed to use assumed name to join the proxy signing interaction) in the reporting procedure, and the more detailed analysis is stated in the next section. Considering the future network environment and the improvement of the quantum technique, we design a new proxy signature scheme based on the module lattice.

According to the table of related work, we compare our work with these works. Our scheme uses blockchain technology to ensure that the honest reporter in our system can be protected and the malicious reporter can be traced. However, all these works cannot achieve this destination. Our scheme uses the proxy signature to achieve the electronic reporting, but works [3–5, 16, 20] use other signature types. The most important thing is that our scheme can resist the attack from the quantum adversary while no one else can.

5.2. System Initialization. Since our scheme is based on the module lattice, by taking the secure parameter 1^λ as input, the procedure first generates the system parameters, such as $\rho, \gamma_1, \gamma_2, \beta, k, l, q, \eta$, and the system functions, such as HighBits() and LowBits(). After obtaining the necessary information, users in our scheme (including the reporter, proxy signer, the electronic reporting box, and "reporting center") can use them to generate their public keys and secret keys. The key generation algorithm KeyGen() is illustrated in Algorithm 1. It first generates a $k \times l$ matrix A , each of which is a polynomial in the ring $R_q = \mathbb{Z}_q[X]/(X^n + 1)$. For the value of q and n, they are restricted tightly in [24]. The secret keys s and e are sampled randomly, and each coefficient of these key vectors is an element from R_q. The size of each coefficient is $\in\in[-\eta, \eta]$. According to the hard assumptions MLWE, the public key is computed as $t = As + e$. Then, users broadcast their public key pk in the blockchain. The public key and secret key can be used to encrypt/decrypt the transiting message among all users and sign/verify for the reporting message.

5.3. Proxy Signing Procedure. Suppose user i is a reporter, user j is the proxy signer, user b is the electronic reporting box, and user a is the "reporting center," and the notations are listed in Table 2:

The proxy signing procedure contains 3 parts: identity authentication, proxy signing, and signature return and is introduced in Figure 2:

(i) *Identity Authentication*. The reporter first randomly selects a vector y_i denoted by $S^l_{\gamma_1 - 1}$ where each coefficient of y_i should be less than $\gamma_1 - 1$. Then, he computes $w_i = Ay_i$ as the temporary key, and in order to be convenient and suitable for the next steps, he uses the function HighBits() to extract the high-order bits of w_i, named as w_{i1}. w_{i1} should satisfy the equation $w_i = w_{i1} \cdot 2\gamma_2 + w_{i0}$ where $w_{i0} \leq \gamma_2$. The reporter hashes the value of w_{i1} as the challenge c_i which consists of 60's $\{-1, 0, 1\}^*$. For the size of the challenge, consider that c_i at most contains 60's ± 1. To make a complete identified authentication, the reporter should "mix" the challenge c_i with her/his own secret key s_i. However, since $s_i \leq \eta$, the size of $c_i s_i$ is less than 60η. β is the maximum coefficient value of $c_i s_i$. Thus, the above condition can be written as $\beta \leq 60\eta$. The authentication requirement is $u_i = y_i + c_i s_i$, but u_i has the limited range of size where $u_i \leq \gamma_1 - \beta$. Besides, to achieve the following authentication, another limitation should be admitted, i.e., the low-order bits of $Ay_i - c_i e_i$'s coefficients should be less than $\gamma_2 - \beta$; otherwise, it will leak the information of the secret key. If the size check passed, the reporter sends (u_i, c_i, M) to the proxy signer. After receiving these information, the proxy signer identifies the reporter by using the function HighBits(). If the reporter's identity is confirmed, the proxy signing will be carried out next.

Procedure KeyGen()
(1) $A \longleftarrow R_q^{k\times l}$
(2) $(s,e) \longleftarrow S_\eta^l \times S_\eta^k$
(3) $t = As + e$
(4) Return $(pk = (A,t), sk = (s,e))$

Algorithm 1: Key Generation.

Table 2: Notations.

Notation	Meaning
sk_i	sk_i is the reporter's secret key, $sk_i = (s_i, e_i)$
pk_i	pk_i is the reporter's public key, $pk_i = t_i$
sk_j	sk_j is the proxy signer's secret key, $sk_j = (s_j, e_j)$
pk_j	pk_i is the proxy signer's public key, $pk_j = t_j$
sk_b	sk_b is the electronic reporting box's secret key, $sk_b = (s_b, e_b)$
pk_b	pk_b is the proxy signer's public key, $pk_b = t_b$
sk_a	sk_a is the reporting center's secret key, $sk_a = (s_a, e_a)$
pk_a	pk_a is the reporting center's secret key, $pk_a = t_a$
M	M is the signing message
σ	σ is the proxy signature

(ii) *Proxy Signing*. The proxy signer makes u_i as y_j to participate in the following signing procedure. Similar as the above process, the proxy signer computes $w_j = Ay_j$ as the signing temporary key and takes the high-order bits w_{j1} of w_j. c_j is hashed from w_{j1} and the signing message M. Since the hash function of the signing procedure is the same as the identity authentication's, the size of $c_j s_j$ is also less than 60η, and the maximum coefficient value of $c_j s_j$ also is written as β where $\beta \le 60\eta$. Thus, the potential signature z_j is constructed by $z_j = y_j + c_j s_j$. In order to protect the secret key and make the signature independent of the secret key, $z_j \le \gamma_1 - \beta$ and also $LowBits(Ay_i - c_j e_j, 2\gamma_2)_\infty \le \gamma_2 - \beta$ which confirms that the signature can be verified validity.

(iii) *Signature Return*. After z_j passes the size check, the proxy signer obtains the proxy signature $\sigma = (z_j, c_j, c_i)$ and sends it to the reporter and the electronic reporting box.

It is stated that to protect privacy, the information should be encrypted by using the destination's public key during the interaction.

5.4. Reporting Record. After receiving the proxy signature, to record this reporting behavior in case of malicious reporting (since the reporter is able to use the assumed name to accomplish the reporting), the reporter should send her/his own secret key sk_i and her/his real name with the signature σ to the trusted third party, named as reporting center. The reporting center stores the information secretly and only broadcasts malicious user's real identity if he tells lies in reporting procedure.

Besides, the electronic reporting box receives the signature and matches it to the previously broadcast public key. The reporting box records the signature with its corresponding public key and waits for permission to verify the reporting center. If the reporting box has not received permission to verify for a long time (The time is set according to the blockchain latency), he will abandon this signature and mark this proxy signer. If the amount of marked users is over the half users of this system, this proxy signer will be broadcast as a malicious user and removed.

5.5. Verification. The electronic reporting box first communicates with the reporting center to confirm whether this signature has been registered or not. The verification is operated by the reporting box after getting permission from the reporting center and is illustrated in Algorithm 2. The reporting box first checks the size of z_j and verifies whether the signature is changed or not during the transmission. According to $Az_j - c_j t_j = Ay_j - c_j e_j$ and $w_j = Ay_j$, it can be written as follows.

$$Az_j - c_j t_j = w_j - c_j e_j. \tag{1}$$

Thus, it is clear that

$$\text{HighBits}\left(Az_j - c_j t_j\right) = \text{HighBits}\left(w_j - c_j e_j\right). \tag{2}$$

Because $\text{LowBits}(Ay_j - c_j e_j, 2\gamma_2)_\infty \le \gamma_2 - \beta$ and the coefficients of $c_j e_j$ are less than β, adding other low-order coefficients cannot cause a big effect in high-order bits. Therefore, the above equations can be written as follows:

$$\text{HighBits}\left(Az_j - c_j t_j\right) = \text{HighBits}\left(w_j - c_j e_j\right) = \text{HighBits}\left(w_j\right). \tag{3}$$

If the hash value of $\text{HighBits}(Az_j - c_j t_j)$ and the signing message is equal to signature's c_j, the signature is not changed during the transmission and is verified validity. Up to here, the reporting box has verified that the signature is generated by the proxy signer and will verify whether the real signer of the signature is the reporter or not.

The verifying process is similar to the above. The reporting box writes $u_{\mathbf{i}}^{'}$ as the result of $Az_j - c_j t_j$. In the function HighBits(), $c_j e_j$ cannot affect the result of the computation. $u_{\mathbf{i}}^{'}$ can be approximately seen as Ay_j, in other words, Au_i. Therefore, use the reporter's public key t_i to identify who the real signer is. Since $u_i' - c_i t_i = Au_i - c_i t_i$ and refer to the above equations, it is clear that

$$\begin{aligned}\text{HighBits}\left(u_i' - c_j t_j\right) &= \text{HighBits}\left(Au_i - c_i t_i\right) \\ &= \text{HighBits}\left(Ay_i - c_i e_i\right).\end{aligned} \tag{4}$$

Besides, since the coefficients of $c_i e_i$ are less than β, adding other low-order bits cannot influence the high-order's. According to the above analysis, if $H(\text{HighBits}(u_i' - c_i t_i)) = c_i$, it can prove that the reporter is the real signer, and the signing message can be accepted by the reporting box while the one-time proxy reporting procedure ends up.

The electronic reporting box verifies the proxy signatures from the proxy signer and collects the reporting message if signatures are valid. For the person who is reported, suppose

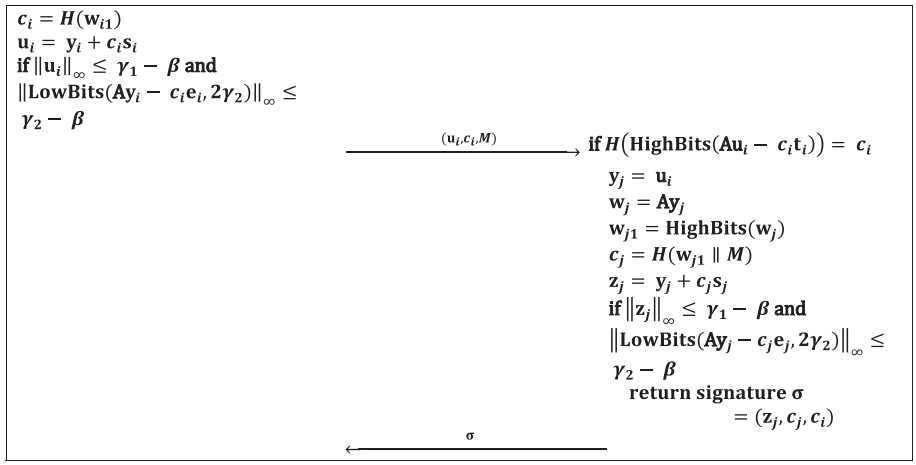

Figure 2: Proxy signing procedure.

Procedure verify (pk_i, pk_j, σ, M)
(1) if $z_{j\infty} \le \gamma_1 - \beta$ and $c_j = H(\text{HighBits}(Az_j - c_j t_j) \| M)$ **then**
(2) compute $u_i' = Az_j - c_j t_j$
(3) if $H(\text{HighBits}(u_i' - c_i t_i)) = c_i$ then
(4) **Return** 1

Algorithm 2: Verification.

that she/he is user m, she/he will not be removed from this blockchain system right away. Only when the amount of signing message is over the half of the blockchain system users, the reporting center will broadcast the message "User m is the traitor, do not trust her/him" and remove user m right away.

6. Security Analysis

According to the adversary model, our scheme can resist these risks:

(1) Suppose an adversary $\mathcal{A}$ who wants to steal the privacy of the reporter. Since the reporter should send reporting center her/his privacy with the signature to register herself/himself, $\mathcal{A}$ wants to steal some information from the transmission. However, our scheme state that any transiting message should be encrypted by using receiver's public key, and the public key is generated based on the hard assumption of MLWE while the encryption in our scheme is Crystals-Kyber [25], one of the Round 3 NIST public-key encryption submissions (Because the main idea of our work is the reporting system designing, the encryption process is omitted). The above encrypted algorithm has postquantum property. Although $\mathcal{A}$ can intercept the ciphertext, she/he is not able to obtain the real message without the reporting center's private key or using modern technology. For the reporting center, she/he is the trusted third party, and only she/he can have access to visit the records of reporter's privacy so that $\mathcal{A}$ cannot get the reporter's privacy there. Thus, our scheme can avoid the risk of reporter's privacy leakage.

(2) Another risk is that the signature misses the required authentication, which means that the signature may not be the reporter's real proxy signature.

Suppose that the proxy signer is malicious, she/he sends a false signature and claims that the signature is entrusted by the reporter, i.e., she/he frame the reporter. Because of the procedure of report recording, our scheme can prevent this risk. In our scheme, the proxy signer should also send the signature back to the reporter so that the reporter will not get the signature if she/he has not submitted the requirement of reporting signature to the proxy signer. Thus, when the proxy signer sends the signature to the electronic reporting box, the framed user will not send her/his privacy information to the reporting center such that the reporting center will not send the permission of verifying to the electronic reporting box and the verifying process will not start. If reporting box does not receive permission to verify for a long time, she/he will mark the proxy signer. When the amount of this proxy signer's marks is over the established domain (here, we set the domain value as half of the system's users), this proxy signer will be removed.

Another case is the user impersonates others to communicate with the proxy signer. However, it is impossible since strict identity authentication is implemented during the interaction and the user cannot obtain other's secret key.

Therefore, our scheme can prevent users from being framed.

(3) Suppose a malicious user $\mathcal{U}$ submits a false reporting message to the proxy signer. Although the false reporting message can finally be signed by the proxy signer, people reported will be removed only when the amount of reporting messages from different

users is over no less than half of all users. Besides, once the reporting message needs to be broadcast after the signature is verified validity, other people will know who has been reported and they can dispute this message with the reporting center if people reported are not bad. If half of the users raise disputes for this reporting message, reporting center will search the signature records to find out the reporter. The reporter can use the assumed name to report others, but she/he has to send his private information (including her/his real name) to reporting center so that reporting center can trace her/his identity and broadcast it. That is, our scheme can find out the malicious user.

7. Conclusions

In this paper, we propose a decentralized electronic reporting scheme based on proxy signature and blockchain and provide the system model of our scheme. To resist the future quantum attack, we propose a new proxy signature based on the module lattice. While preserving the reporter's privacy, our scheme can trace the malicious users at the same time, which greatly improves the usability of our scheme. Besides, we give a detailed security analysis for the adversary model. In the future, we will improve our proposed system efficiency and make the comparison with other electronic reporting systems. [13–15, 23].

Data Availability

The signature data and the code used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The research was financially supported by the Foundation of Yunnan Key Laboratory of Blockchain Application Technology (Nos. 202105AG070005 and YNB202103), the National Natural Science Foundation of China (No. 61972366), the Provincial Key Research and Development Program of Hubei (No. 2020BAB105), and the Foundation of Guizhou Provincial Key Laboratory of Public Big Data (No. 2019BDKFJJ003 and 2019BDKFJJ011).

References

[1] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for delegating signing operation," in *Proceedings of the 3rd ACM Conference on Computer and Communications Security*, pp. 48–57, New Delhi, India, January 1996.

[2] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures: Delegation of the power to sign messages," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 79, no. 9, pp. 1338–1354, 1996.

[3] Y. Wang, W. Qiu, L. Dong et al., "Proxy signature-based management model of sharing energy storage in blockchain environment," *Applied Sciences*, vol. 10, no. 21, p. 7502, 2020.

[4] H. Shen, J. Zhou, Z. Cao, X. Dong, and K.-K. R. Choo, "Blockchain-based lightweight certificate authority for efficient privacy-preserving location-based service in vehicular social networks," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6610–6622, 2020.

[5] M. Pawlak, A. Poniszewska-Marańda, and J. Guziur, "Intelligent agents in a blockchain-based electronic voting system," in *Proceedings of the Intelligent Data Engineering and Automated Learning – IDEAL 2018. IDEAL 2018. Lecture Notes in Computer Science*, vol. 11314, 2018.

[6] X. Jia, H. Yupu, and J. Mingming, "Lattice-based forward secure proxy signatures," *Journal of Computer Research and Development*, vol. 58, no. 3, p. 583, 2021.

[7] R. Gao and J. Zeng, "Forward secure certificateless proxy multi-signature scheme," *International Journal of Electronic Security and Digital Forensics*, vol. 13, no. 1, pp. 1–27, 2021.

[8] R. Huang, Z. Huang, and Q. Chen, "A generic conversion from proxy signatures to certificate-based signatures," *Journal of Internet Technology*, vol. 22, no. 1, pp. 209–217, 2021.

[9] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: a distributed solution to automotive security and privacy," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 119–125, 2017.

[10] E. Bellini, Y. Iraqi, and E. Damiani, "Blockchain-based distributed trust and reputation management systems: a survey," *IEEE Access*, vol. 8, pp. 21 127–21 151, 2020.

[11] S. Yu, K. Lv, Z. Shao, Y. Guo, J. Zou, and B. Zhang, "A high performance blockchain platform for intelligent devices," in *Proceedings of the 2018 1st IEEE international conference on hot information-centric networking (HotICN)*, pp. 260-261, IEEE, Shenzhen, China, August 2018.

[12] W. Liang, Y. Fan, K.-C. Li, D. Zhang, and J.-L. Gaudiot, "Secure data storage and recovery in industrial blockchain network environments," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6543–6552, 2020.

[13] W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han, and C. Su, "Blockchain-based reliable and efficient certificateless signature for iiot devices," *IEEE Transactions on Industrial Informatics*, p. 1, 2021.

[14] H. Xiong, C. Jin, M. Alazab et al., "On the design of blockchain-based ecdsa with fault-tolerant batch verication protocol for blockchain-enabled iomt," *IEEE Journal of Biomedical and Health Informatics*, p. 1, 2021.

[15] T. R. Gadekallu, Q. V. Pham, D. C. Nguyen et al., "Blockchain for edge of things: Applications, opportunities, and challenges," *IEEE Internet of Things Journal*, vol. 9, no. 2, p. 1, 2021.

[16] Y. Chen, J. Sun, Y. Yang, T. Li, X. Niu, and H. Zhou, "PSSPR: a source location privacy protection scheme based on sector phantom routing in WSNs," *International Journal of Intelligent Systems*, vol. 7, no. 2, pp. 1204–1221, 2022.

[17] T. Li, Z. Wang, Y. Chen, C. Li, Y. Jia, and Y. Yang, "Is semi-selfish mining available without being detected?" *International Journal of Intelligent Systems*, 2021.

[18] B. Wang, J. Sun, Y. He, D. Pang, and N. Lu, "Large-scale election based on blockchain," *Procedia Computer Science*, vol. 129, pp. 234–237, 2018.

[19] S. A. Adeshina and A. Ojo, "Maintaining voting integrity using blockchain," in *Proceedings of the 2019 15th International Conference on Electronics, Computer and Computation (ICECCO)*, pp. 1–5, IEEE, Abuja, Nigeria, December 2019.

[20] H. Wang, D. He, Z. Liu, and R. Guo, "Blockchain-based anonymous reporting scheme with anonymous rewarding," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1514–1524, Nov. 2020.

[21] W. Qiu, B. Liu, and S. Shi, "An impeaching system based on bit commitment with revocable anonymity," in *Proceedings of the 2010 International Conference on Internet Technology and Applications*, pp. 1–6, IEEE, Wuhan, China, August 2010.

[22] S. Zou, J. Xi, S. Wang, Y. Lu, and G. Xu, "Reportcoin: a novel blockchain-based incentive anonymous reporting system," *IEEE Access*, vol. 7, pp. 65544–65559, 2019.

[23] M. Ajtai, "Generating hard instances of lattice problems," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing*, pp. 99–108, Pennsylvania, Philadelphia, USA, July 1996.

[24] M. Ajtai and C. Dwork, "A public-key cryptosystem with worst-case/average-case equivalence," in *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, pp. 284–293, Texas, El Paso, USA, May 1997.

[25] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," in *Proceedings of the 2014 USENIX Annual Technical Conference (USENIX ATC 14)*, pp. 305–319, USENIX Association, Philadelphia, PA, June 2014, https://www.usenix.org/conference/atc14/technical-sessions/presentation/ongaro.

[26] L. Ducas, E. Kiltz, T. Lepoint et al., "CRYSTALS-dilithium: a lattice-based digital signature scheme," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2018, no. 1, pp. 238–268, 2018.

[27] J. Bos, L. Ducas, E. Kiltz et al., "Crystals - kyber: a cca-secure module-lattice-based kem," in *Proceedings of the 2018 IEEE European Symposium on Security and Privacy (EuroS P)*, pp. 353–367, London, UK, April 2018.

[28] T. R. Gadekallu, Q. V. Pham, D. C. Nguyen et al., "Blockchain for edge of things: Applications, opportunities, and challenges," *IEEE Internet of Things Journal*, vol. 9, no. 2, pp. 964–988, 2021.

[29] A. Langlois and D. Stehlé, "Worst-case to average-case reductions for module lattices," *Designs, Codes and Cryptography*, vol. 75, no. 3, pp. 565–599, 2015.