Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.037796
Article

Quantum Secure Undeniable Signature for Blockchain-Enabled Cold-Chain Logistics System

Chaoyang Li, Hongxue Shen, Xiayang Shi and Hui Liang*

College of Software Engineering, Zhengzhou University of Light Industry, Zhengzhou, 450001, China
*Corresponding Author: Hui Liang. Email: hliang@zzuli.edu.cn

Received: 16 November 2022; Accepted: 08 February 2023

Abstract: Data security and user privacy are two main security concerns in the cold-chain logistics system (CCLS). Many security issues exist in traditional CCLS, destroying data security and user privacy. The digital signature can provide data verification and identity authentication based on the mathematical difficulty problem for logistics data sharing in CCLS. This paper first established a blockchain-enabled cold-chain logistics system (BCCLS) based on union blockchain technology, which can provide secure data sharing among different logistics nodes and guarantee logistics data security with the untampered blockchain ledger. Meanwhile, a lattice-based undeniable signature scheme is designed to strengthen the security of logistics data and user privacy against quantum attacks. This scheme is based on the lattice assumption, which can provide anti-quantum security for BCCLS in the future quantum computer age. It also establishes the undeniable mechanism that guarantees that the actual signer cannot deny a valid signature. Then, security proof shows that this undeniable signature scheme is correct and safe, and an efficiency comparison shows that it is more efficient than other schemes in similar literature. The performance evaluations of transaction throughput and latency show that the proposed BCCLS is efficient and practical. This work can improve the security and efficiency of logistics data management and promote the reform and development of the logistics industry.

Keywords: Undeniable signature; cold-chain logistics system; blockchain; privacy-preserving

1 Introduction

Nowadays, the development of e-commerce promotes the rise and prosperity of the logistics industry. Cold-chain logistics is an essential part of the current logistics industry, which guarantees the transportation process safety for frozen food [1]. However, many food security affairs exist in centralized CCLSs as their managers can easily change the logistics data. The centralized storage form quickly leads to data loss once the storage server has been destroyed by a hacker or a natural disaster

[2]. Therefore, more secure storage forms have been sought by academia and industry researchers with the technologies of cloud computing, blockchain, and artificial intelligence.

Blockchain technology shows more potential applications to promote the transformation and upgrading of current information systems, such as financial [3], healthcare [4,5], and the Internet of things (IoT) [6,7]. It also has a more promising function to change the traditional centralized CCLS. Some blockchain-based distributed logistics data management systems have been introduced, such as Blockcoldchain [8] and ColdBlocks [9]. These BCCLSs successfully solve the data loss and information leakage problems in traditional centralized systems. The open and transparent blockchain ledger takes the security assurance for logistics data and the tamper-free capability for operation records. Frozen food safety is related to people's life and health, and the authenticity and reliability of logistics data in CCLS are the critical factors in guaranteeing food safety [10]. BCCLS can provide a secure logistics data management platform and establish a logistics data sharing mechanism among different logistics nodes. Data transparency and centralization are more conducive to the frozen food safety and data value exploitation. However, with the expansion of the frozen food market and the increase in users, transaction processing needs a more efficient and secure transaction verification algorithm [11]. Meanwhile, preventing the denial of the transaction signature is critical to reducing food safety incidents and disputes.

Facing the security demand of BCCLS, some cryptographic algorithms can improve the security of data transactions and identity privacy. The signature algorithms in many current information systems are based on complex mathematic problems, such as large integer decomposition, discrete logarithm, and elliptic curves discrete logarithm [12]. These algorithms are secure and efficient in the classical computing environment, but they are not safe in the quantum computing environment. Therefore, it is urgent to explore anti-quantum algorithms, such as lattice cryptography [13,14], hash cryptography [15], and code-based cryptography [16]. The BCCLS also needs a more secure signature algorithm to resist quantum attacks empowered by the quantum computer. Depending on these quantum secure foundational cryptographic algorithms, some anti-quantum digital signature schemes have been introduced, such as blind signature [17,18], group signature [19], undeniable signature [20], and so on. Every kind of digital signature can provide one particular function. This paper mainly focuses on the logistics data repudiation problem and seeks a more secure and efficient undeniable signature scheme.

Hence, this paper introduces a distributed BCCLS to establish a logistics data secure sharing platform and designs an undeniable signature scheme to strengthen data and user privacy security. Here, the detailed contributions are summarized as following.

- A distributed BCCLS based on union blockchain technology has been established, which contains all the related parties from generation to consumption of frozen food. This system utilized the public and untampered blockchain ledger to achieve secure logistics data management and sharing between different parties.
- An undeniable signature scheme has been designed to strengthen data and user privacy security. Based on this scheme, the transaction parties do not deny the transaction data signed with their signatures, and this signature can also provide identity authentication for the legal system user. Meanwhile, which has anti-quantum attack property with lattice assumption.
- The efficiency comparison results show that the proposed undeniable signature scheme is more efficient than similar protocols. Equipping with this signature, the performance evaluations of transaction throughput (TPS) and transaction latency (TL) show that the BCCLS is secure, stable, and practical.

In the following, Section 2 gives the descriptions of BCCLS; Section 3 introduces the proposed blockchain-enabled cold-chain logistics system; Section 4 presents the protocol description and security proof of the lattice-based undeniable signature scheme; Section 5 shows the efficiency comparison and performance evaluation; Last Section 6 provides the conclusion.

2 Related Work

Because of the security issues in CCLS, this section reviews the latest research progress about the novel blockchain-based framework and related security issues.

2.1 Distributed CCLS with Blockchain

With the deepening application in IoT, blockchain shows a very promising application in CCLS. Some distributed CCLSs have been proposed based on blockchain technology to change the centralized management form in traditional systems. Kim et al. applied the Hyperledger fabric to establish a BCCLS for blood transactions among medical institutions [21]. Mendonça et al. designed a Blockcoldchain platform for a vaccine cooling track facing the COVID-19 pandemic, which could provide public and verifiable logistics records [8]. Menon et al. proposed an IoT-blockchain for quality assurance in CCLS, and it established an immutable and decentralized database to store the logs transactions [9]. Khan et al. reviewed the applications, challenges, and future blockchain technology trends for drug delivery in CCLS [7]. Si presented a multi-mode blockchain data model for agriculture and adopted an off-chain storage method to lighten the redundancy of an online ledger [22]. Hu developed a real-time monitoring system for CCLS based on IoT, blockchain, and computer technologies, and this system can grasp the real-time dynamics data to adjust the conditions [23]. These papers design various BCCLSs for cold-chain logistics data management and focus on data collection and storage. However, the overall process of data management and sharing is rarely considered in these protocols. Therefore, this paper plans to establish a distributed BCCLS for frozen food delivery, which can achieve logistics data supervision from generation to consumption.

2.2 Security Mechanism and Algorithm

Cryptographic algorithms are the main methods to protect system data and privacy information for CCLSs. Pan et al. proposed a deep neural network to accomplish signature classification for non-orthogonal multiple access in the future Internet of Things (IoT) [24]. Li et al. designed a decentralized attribute-based signature scheme to weaken centralized management, resource consumption, and illegal access in traditional IoT systems [25]. Huang et al. introduced a certificateless group signature scheme for data package authentication in mobile edge computing [26]. However, these former signature schemes do not resist quantum attacks which can bring many threats to current cryptographic-based information systems. However, post-quantum algorithms have been introduced recently, and lattice cryptography is a more promising theory to provide anti-quantum security. Li et al. designed an anti-quantum signature scheme with lattice cryptography, which can achieve message blindness [13]. Wang et al. presented an identity-based signature scheme with lattice assumption, which has been applied to strengthen identity authentication in work-from-home (WFH) [14]. Rawal et al. introduced a lattice-based undeniable signature scheme that utilized the challenge-response mechanism to realize signature undeniable [20]. Zhang et al. analyzed the risk factors of medical CCLS and established an adjacency matrix to find the relationship between different factors [27]. Using these security mechanisms and algorithms, the CCLS can provide a comprehensive security guarantee for logistics data and user privacy. Furthermore, the efficiency and anti-quantum property should also be considered for the security of CCLS.

3 Blockchain-Enabled Cold-Chain Logistics System

A distributed BCCLS based on blockchain technology has been presented, which can aggregate the related entities to establish a data management system. Then, an undeniable signature has been applied to this system to improve logistics data security for transaction verification and identity authentication. The framework of this BCCLS is described in Fig. 1.

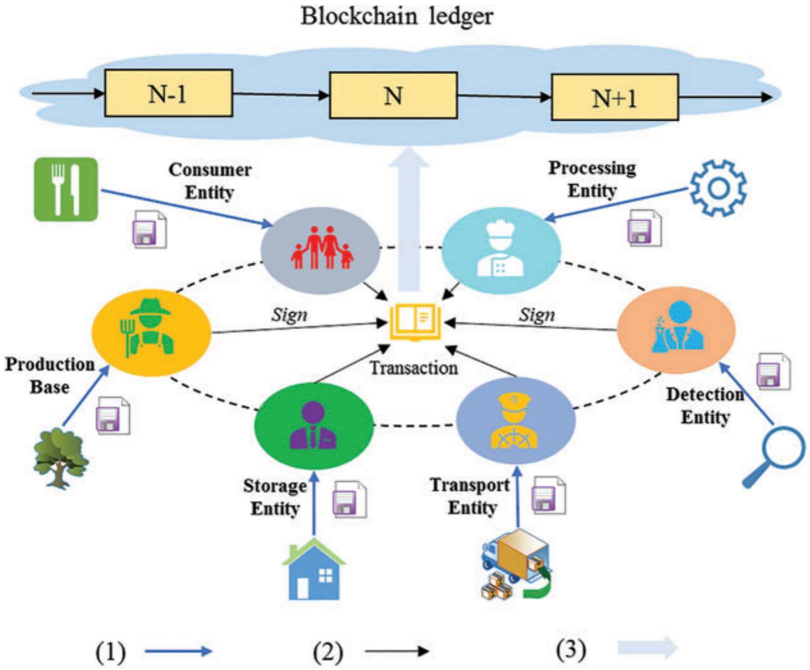

Figure 1: The framework of BCCLS

3.1 System Framework

By utilizing blockchain technology, production base, storage, transport, detection, processing, and consumer entities compose a distributed network for cold-chain logistics data management. The government also can take part in this system as a system node to perform supervisory duties. Meanwhile, a public blockchain ledger has been formed to record the logistics information, transaction data, and processing records. Here, the logistics data should pass the following steps to become the untampered transaction records in the blockchain ledger. (1) The life cycle data of frozen food are collected by the temperature, humidity, and location sensors; (2) All the logistics data and processing records are packaged into different transactions with the operators' signature and timestamp; (3) These packaged transactions accept the verification of BCCLS, and they will be linked to the public blockchain ledger when they pass system consensus process; Then, these data can be transmitted among different cold-chain logistics entities with one unified blockchain ledger of the whole network consensus. This ledger can guarantee data management security and provide evidence for process tracing with the tamper-free mechanism. In addition, these entities' unions also can balance the resource allocation and expand the resource value for the frozen food market. Here, the signature scheme plays two functions: transaction verification and identity authentication.

3.1.1 *Transaction Verification*

The undeniable signature makes it responsible for transaction verification in the BCCLS. As the collected logistics data contain the operator's signature and timestamp, the system node verifies the signature's legality and the processing timeline's rationality. Then, the authenticated logistics data are packaged into one temporary block to be verified by the network-wide node. As shown in Fig. 2, the transactions in the temporary block need to pass the processes of broadcast, verify, feedback, confirm, and public. In this network-wide verification process, the operators perform the following five steps: 1) The leader node broadcasts the transactions to other general nodes; 2) A general node verifies received transactions, signs with their signature, and sends them to other nodes for verification; 3) Other nodes verify, sign, and return them; 4) The general nodes confirm the verification results and return them to the leader; 5) The leader node checks the results and public them to the whole network. In the end, these data have been formed as immutable records in the blockchain ledger when they verify the distributed system and achieve the consensus of the whole network.

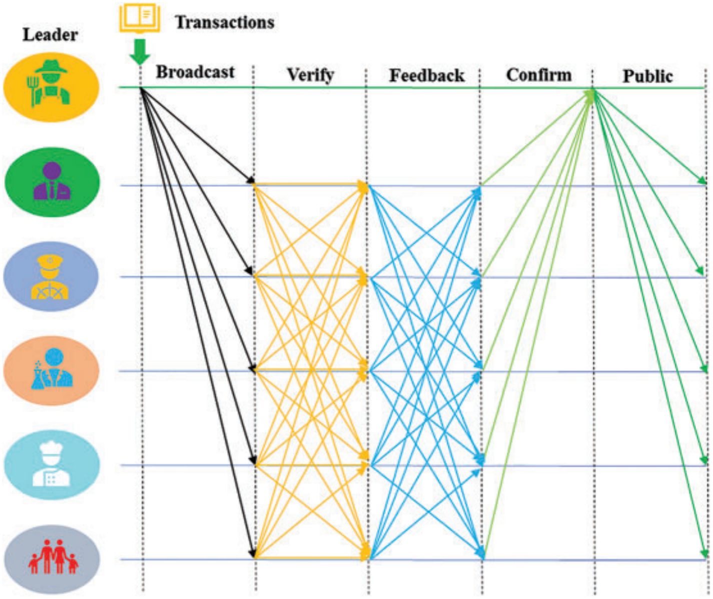

Figure 2: Transaction verification in the BCCLS

3.1.2 *Identity Authentication*

This undeniable signature takes the other responsibility for the identity verification in the BCCLS. The logistics data and processing records contain the operators' signatures, establishing an identity authentication path. This signature is undeniable, and the signer cannot deny the transaction with his signature. The blockchain ledger provides historical data processing records, and this signature guarantees the undenied operational behavior. For example, a consumer can obtain information about complete production, transportation, and operators through the quick response (QR) code or barcode on frozen food packaging. The consumer can check the records' integrity and the transactions' authenticity, whether it is recorded into the blockchain ledger in BCCLS. Here, the signature is used for transaction verification in the system consensus process and identity authentication in the case of record pursuit. Therefore, it establishes a tracing mechanism in a frozen food security incident.

This system is suitable for logistics data management of frozen food, such as the fresh products of meat, vegetable, and fruit, the manufactured food of quick-frozen food, meat, and aquatic products, and the medical products of refrigerated medicines, reagent, and medical devices. Compared with the traditional centralized CCLS, this distributed system establishes a data secure sharing mechanism for frozen food and takes the security guarantee for cold-chain logistics data. Meanwhile, this BCCLS allows the joining and leaving of cold-chain logistics nodes, which provides a public platform for cold-chain logistics data sharing and management. It also helps to aggregate the scattered cold-chain logistics data and promote the value of these data. Next, a detailed description of the lattice-based undeniable signature scheme is presented, while its security proof is given in the following.

4 Lattice-Based Undeniable Signature Scheme

This signature scheme is designed with the short integer solution (SIS) problem $\mathbb{Z}-SIS^{\kappa}_{q,n,m,\beta}$ based on the number theory research unit (NTRU) lattice [28]. Here, the SIS problem cannot be cracked with classical or quantum computers. Meanwhile, the system vectors are selected by bimodal Gaussian distribution which is a randomized nearest-plane algorithm on $D_{\Lambda,c,\sigma}$ with relation to lattice Λ [29]. Table 1 shows the symbol definition of some essential parameters used in the following sections.

Table 1: Symbol definition

Items	Meaning
$\mathbb{Z}$	Collection space of lattice base.
n, m	Size of the keys' matrix.
q	Modulus of the matrix.
κ	System security parameter.
σ	System parameter.
h_1, h_2	Hash function.
A, S	The public key and private key.
msg	The message.
$e \to (e_1, e_2, e_3)$	The signature of message msg.

4.1 Protocol Description

This undeniable signature scheme contains four steps, **KeyGen.**, **SigGen.**, **Verify**, and **Confirmation/Disavowal**, and the detailed scheme model is shown in [30]. The simple workflow is shown in Fig. 3, and the detailed descriptions of these four steps are given below.

KeyGen. $n, m, q \to (A \in \mathbb{Z}_{2q}^{n*m}, S \in \mathbb{Z}_{2q}^{m*n})$: According to the rules in [9], parameters n, m, q, κ, σ are defined. Note that κ is the security parameter, parameter m satisfies $m = O(n \log q)$, and two hash functions are defined as $h_1 : \{0,1\}^* \to \mathbb{Z}_{2q}^{n*m}$ and $h_2 : \{0,1\}^* \to \{v : v \in \{-1,0,1\}^k, ||v|| \leq k\}$. Then, system keys are generated by the following steps:

- Chose a short matrix $S \in \mathbb{Z}_{2q}^{m*n}(||\widetilde{S}|| \leq O\left(\sqrt{n \log q}\right)$ and $||S|| \leq O(n \log q))$, and set it as the secret key;

- Compute $A \in \mathbb{Z}_{2q}^{n*m}$ $(AS = A(-S) = qI_n(\mathrm{mod}2q))$, and set it as the public key;
- Chose a random seed sd, and calculate $\mathrm{H} = h_1(sd)$;
- Chose a random vector $x \leftarrow D_{\sigma}^{m}$, and calculate $\mathrm{X} = \mathrm{H}x^T\mathrm{mod}2q$;
- Output the $(A, \mathrm{H}, \mathrm{X})$, and keep (S, x) secretly.

SignGen. $\{(A, \mathrm{H}, \mathrm{X}), (S, x)\} \rightarrow e$: Given the message msg, the signer performs the following steps to generate a signature.

- Computes $\mathrm{M} = h_1(msg)$;
- Computes $e_3 \leftarrow \mathrm{M}x^T\mathrm{mod}2q$;
- Computes $e_1 \leftarrow h_2(\mathrm{X} + Ay\mathrm{mod}q, \mathrm{M})$;
- Computes $e_2 \leftarrow y + e_1S$;
- Outputs the signature $e \rightarrow (e_1, e_2, e_3)$.

Verify (msg, e): Verifier first checks the validity of pair (e_1, e_2). Here, denoting $W = \eta\sqrt{m}\sigma$, one can set η so that $||w_i|| > W$ is verified with probability $1 - 2^{-\kappa}$ for the security parameter κ (in practice $\eta \in [1.1, 1.4]$).

- If $||e_2|| > W$ or $||e_2||_\infty > q/4$, then outputs *Reject*;
- Checks $e_1 \leftarrow h_2(\mathrm{X} + Ae_2 - qe_1\mathrm{mod}2q, \mathrm{M})$, otherwise outputs *Reject*.

Confirmation/Disavowal $e \rightarrow$ (*Reject* or *Accept*): The signer and verifier perform the following steps to verify the validity of e_3.

- Signer and verifier execute the hash function h_1 to calculate H and M;
- Signer selects permutation π over $(1, 2, \ldots, m)$ and $u \in \mathbb{Z}_q^m$, and then he calculates $C_1 = h_1(\pi||\mathrm{H}u^T\mathrm{mod}2q)$, $C_2 = h_1(\pi(u))$, $C_3 = h_1(\pi(u + x))$, and $C_4 = h_1(\pi||\mathrm{M}u^T\mathrm{mod}2q)$ as his commitments;
- Verifier sets a challenge $c \in \{0, 1, 2\}$ and sends it to signer.
- Signer answers the challenge c according the following rulers:
  1) Returns π and u for the challenge $c = 0$;
  2) Returns π and $u + x$ for the challenge $c = 1$;
  3) Returns $\pi(\mathrm{u})$ and $\pi(x)$ for the challenge $c = 2$.
- Verifier verifies the commitments when he has received the responses:
  1) For the challenge $c = 0$, verifier verifies whether the commitments C_1,C_2 , and C_4 are correct or not;
  2) For the challenge $c = 1$, verifier verifies whether the commitments C_1,C_3 , and the validity of C_4. When $C_4 = h_1(\pi||\mathrm{M}(u+x)^T - e_3\mathrm{mod}2q)$, it is confirmation; otherwise, it is disavowal;
  3) For the challenge $c = 2$, verifier verifies the validity of C_2,C_3 and $||\pi\ (e)|| \leq \beta\sqrt{m}$.

Then, the verifier announces the signature is valid and accepts it when all the challenges have passed his verification.

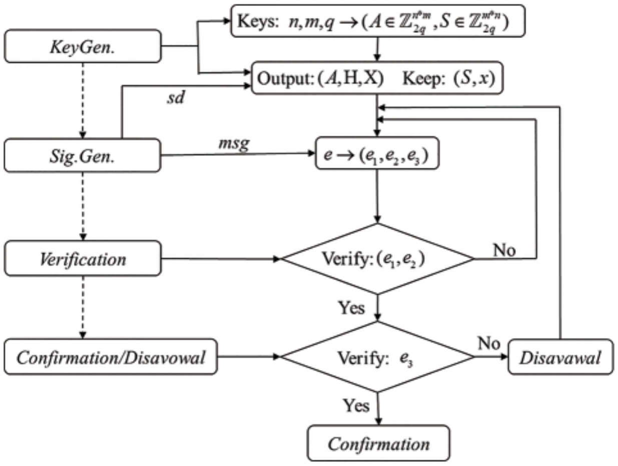
KeyGen.
Keys: $n,m,q \rightarrow (A \in \mathbb{Z}_{2q}^{n*m}, S \in \mathbb{Z}_{2q}^{m*n})$
Output: $(A,\mathrm{H},\mathrm{X})$ Keep: (S,x)
sd
Sig.Gen.
msg
$e \rightarrow (e_1,e_2,e_3)$
Verification
Verify: (e_1,e_2)
No
Yes
Confirmation/Disavowal
Verify: e_3
No
Disavawal
Yes
Confirmation

Figure 3: Workflow of the proposed undeniable signature scheme

4.2 Security Proof

For the proposed signature scheme, the correctness, soundness and unforgeability are three main security items that must be proved. The detailed analyses of these three security properties are reduced to the following three theorems.

Theorem 1 *Correctness*: The message and signature pair (msg, e) is valid with $Prob(\text{Confirmation}) = 1$ when the signer and verifier perform honestly. Otherwise, an invalid pair (msg, e) is with $Prob(\text{Disavowal}) = 1$.

Proof: For a valid (msg, e), there have

$$(\mathrm{H}(u + x)^T - \mathrm{X}) = (\mathrm{H}u^T + \mathrm{H}x^T - \mathrm{X}) = \mathrm{H}u^T \mathrm{mod}2q \tag{1}$$

$$(M(u + x)^T - e_3) = (Mu^T + Mx^T - e_3) = Mu^T \mathrm{mod}2q \tag{2}$$

$$\pi(x) + \pi(u) = \pi(x + u) \tag{3}$$

Then, it can derive

$$C_1 = h_1(\pi||(\mathrm{H}(u + e)^T - \mathrm{X})\mathrm{mod}2q) \tag{4}$$

$$C_3 = h_1(\pi(x) + \pi(u)) \tag{5}$$

$$C_4 = h_1(\pi||M(u + x)^T - e_3 \ \mathrm{mod}2q) \tag{6}$$

Here, C_1,C_2 and C_4 are honestly worked out, the pair (msg, e) is accepted with $Prob(\text{Confirmation}) = 1$.

Otherwise, $e_3 \neq \mathrm{M}x^T \mathrm{mod}2q$ with an invalid pair (msg, e). So $C_4 \neq h_1(\pi||M(u + x)^T - e_3\mathrm{mod}2q)$, and the pair (msg, e) is denied with $Prob(\text{Disavowal}) = 1$.

Theorem 2 *Soundness*: For an invalid message and signature pair (msg, e), the probability of $Prob(\text{Disavowal})$ is close to 1; Otherwise, the probability of $Prob(\text{Confirmation})$ is close to 1 if (msg, e) is valid.

Proof: Assuming (msg, e) is an invalid message and signature pair, there exists $e_3 \neq \mathrm{M}x^T \mathrm{mod}2q$. The signer still responds to the challenges according the principle, and the responses are as following.

(1) if $c = 0$, sends ϕ_1 and θ_1;

(2) if $c = 1$, sends ϕ_1 and θ_2;
(3) if $c = 2$, sends θ_3 and θ_4;

Next, the verifier can derive:

$$C_1 = h_1(\phi_1||\mathrm{H}\theta_1^T\mathrm{mod}2q) = h_1(\phi_1||(\mathrm{H}\theta_2^T - \mathrm{X})\mathrm{mod}2q) \tag{7}$$

$$C_2 = h_1(\phi_1(\theta_1)) = h_1(\theta_4) \tag{8}$$

$$C_3 = h_1(\phi_1(\theta_2)) = h_1(\theta_3 + \theta_4) \tag{9}$$

$C_4 = h_1(\phi_1||M\theta_1^T\mathrm{mod}2q) = h_1(\phi_1||M\theta_2^T - e_3\mathrm{mod}2q)$. Here, $||\theta_3|| \leq \beta\sqrt{m}$. Note h_1 is defined as a random hash oracle function, so it can derive the following results.

$$\mathrm{H}\theta_1^T\mathrm{mod}2q = (\mathrm{H}\theta_2^T - \mathrm{X})\mathrm{mod}2q \tag{10}$$

$$\phi_1(\theta_1) = \theta_4 \tag{11}$$

$$\phi_1(\theta_2) = \theta_3 + \theta_4 \tag{12}$$

$$M\theta_1^T\mathrm{mod}2q = M\theta_2^T - e_3 \ \mathrm{mod}2q \tag{13}$$

Then, the equations $\theta_4 - \theta_1 = \phi_1^{-1}(\theta_3)$ and $\mathrm{X} = \mathrm{H}\phi_1^{-1}(\theta_3)^T$ hold. Therefore, it has $x = \phi_1^{-1}(\theta_3)$ and $e_3 = \mathrm{M}\phi_1^{-1}(\theta_3)^T\mathrm{mod}2q = \mathrm{M}x^T\mathrm{mod}2q$. However, the invalid pair (msg, e) cannot hold $e_3 = \mathrm{M}x^T\mathrm{mod}q$. This contradiction shows that signer cannot correctly respond the challenges. In the best case, he can answer two challenges with probability $\frac{2}{3}$. When response rounds achieve $N(N \geq 2)$ times, the probability $Prob$(Disavowal) becomes $1 - \left(\frac{2}{3}\right)^N$, and it is more close to 1 with the increasing of N.

Theorem 3 *Unforgeability*: For a secure signature scheme, there is not exist an adversary who can forge a valid signature for the target message by adaptive chosen message attack.

Proof: Assuming that there is an adversary A_0 who has ability to destroy the existentially unforgeability by a non-negligible probability ε, a challenger C can successfully solve the $SIS_{2\beta}$ instance. Then, the adversary A_0 and challenger C perform a query-respond game with relate to the signature scheme. With the public parameters A, sd, and S, C executes the queries on hash algorithm and sign step.

For the queries on hash functions h_1 and h_2, C first checks the local lists $List_{h_1}$ and $List_{h_2}$ whether the message is queried before or not. If there exist (sd, H) and (msg, M), C returns the results back to A_0. Otherwise, C computes $\mathrm{H} = h_1(sd)$ and $\mathrm{M} = h_1(msg)$, returns them back, and stores them into lists $List_{h_1}$ and $List_{h_2}$ respectively.

Next, for the signature query, C also first checks the local list $List_S$. If there exist (msg, e), C returns the results back to A_0. Otherwise, C performs **SignGen.** algorithm, returns (msg_i, e_{msg_i}) back, and stores them into list $List_S$ respectively. Here, A_0 queries on signature with relate to many messages (not the target message). Suppose A_0 can forge a valid signature (msg^*, e^*) based on many query experiences with $e^* = (e_1^*, e_2^*, e_3^*)$. Now, (e_1^*, e_2^*) is valid as the following Eq. (14) holds.

$$\begin{aligned} X + Ae_2 - qe_1 &= X + A(y + e_1S) - qe_1 \\ &= X + Ay + ASe_1 - qe_1 \\ &= X + Ay + qe_1 - qe_1 \\ &= X + Ay \ \mathrm{mod}\ 2q \end{aligned} \tag{14}$$

Therefore, (e_1^*, e_2^*) is derived from queried results, e_3^* is forged by the adversary A_0. There has $e_3^* \neq \mathrm{M}^* x^{*T} \mathrm{mod} q$ with valid e_3^*. Meanwhile, there has $e_3 \neq \mathrm{M}^* x^T \mathrm{mod} q$ as M^* is a result from signature query. It also can derive $e_3^* - e_3 \neq \mathrm{M}^*(x^* - x)^T \mathrm{mod} 2q$, and $||x^* - x|| \leq 2\beta\sqrt{m}$ is a solution for $SIS_{2\beta}$ instance.

5 Comparison and Performance

This section presents the efficiency comparison between the proposed undeniable and similar schemes, and gives the performance evaluation of transactions executed in BCCLS. The results are given below.

5.1 *Efficiency Comparison*

Table 2 presents the comparison results by analyzing with the unified system parameters $(n, m, q, \kappa, \sigma)$. The sizes of the public key (PK) and secret key (SK) in the proposed scheme are equal to that in Ref. [13] and smaller than those in Ref. [14] and Ref. [20]. Meanwhile, Ref. [13] and Ref. [14] cannot achieve the undeniable property. With the same security level, more small key size can make the system more efficient. Although the signature size is more big than that in Ref. [13] and Ref. [14], it can guarantee that the signature is undeniable. Here, λ in Ref. [14] is a positive integer that is chosen by the bimodal Gaussian distribution. Equipped with this undeniable signature, it can establish a data transaction traceability mechanism for food safety incidents' disputes in BCCLS because the signer cannot deny a data transaction with his signature.

Table 2: Comparison results with similar schemes

Scheme	PK size	SK size	Signature size
Ref. [13]	$mn \log 2q$	$mn \log 2q$	$m \log(12\sigma)$
Ref. [14]	$2mn \log q$	$2mn \log q$	$\lambda(\log\kappa + 1) + m \log(12\sigma)$
Ref. [20]	$2mn \log q$	$2mn \log q$	$2m \log q + m \log(12\sigma)$
This scheme	$mn \log 2q$	$mn \log 2q$	$2m \log 2q + m \log(12\sigma)$

5.2 *Performance Evaluation*

The performance evaluations of the proposed BCCLS and undeniable signature scheme are presented in this section.

Firstly, evaluations of the key size are given, which mainly affects the transaction execution efficiency. With the general setting of the SIS problem $\mathbb{Z} - SIS^{\kappa}_{q,n,m,\beta}$, the performance is executed with 80-bit and 192-bit security levels of $N = 512, q = 2^{23}$ and $N = 1024, q = 2^{27}$ respectively. Then, parameter m $(m \geq 2n \lceil \log q \rceil)$ is set as $m = 3549/7807$ for the different two security levels, and parameters λ and κ in Ref. [10] are set as $\lambda = 1.1$ and $\kappa = 28$ with the same rules. Meanwhile, parameter is set as $\sigma = 12, \sqrt{\kappa} = 64$. Then, the performance results are shown in following two figures by comparing with other three schemes, where Fig. 4 shows the comparison results with an 80-bit security level and Fig. 5 is with a 192-bit security level. Although the sizes of PK and SK seem more big than that in the current cryptographic system, they will provide more strong security assurance for information systems in the future quantum age. The computational complexity can also become insignificant with a quantum computer. This undeniable signature scheme has more efficient computational advantages than similar schemes and provides stronger security against classical and quantum attacks. Therefore, the proposed undeniable signature scheme can guarantee the security of the data sharing process through BCCLS.

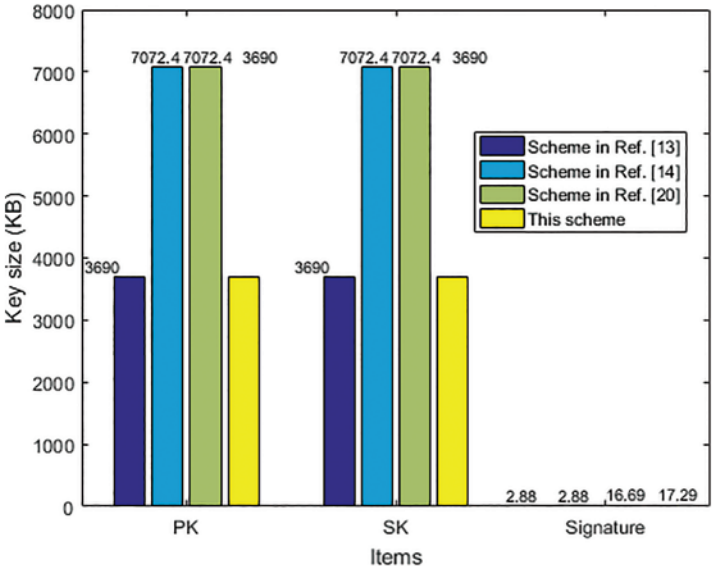

Figure 4: Key size comparison with 80-bit security

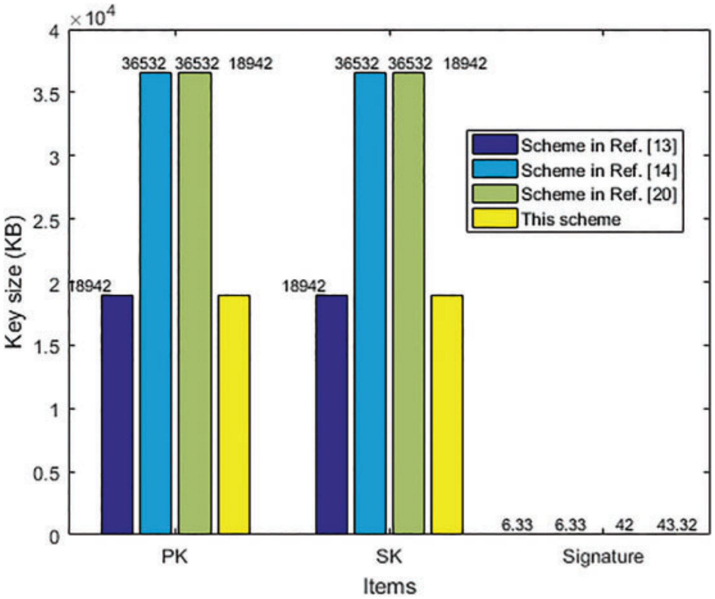

Figure 5: Key size comparison with 192-bit security

Secondly, the performance evaluations concerning TPS and TL for the proposed BCCLS have been presented. Here, TPS is a crucial metric to measure system scalability, and TL is the standard for assessing communication efficiency and operational duration. The performance is executed on the Hyperledger Fabric with the transaction number increasing from 200 to 1200. Then, the following two figures show the evaluation results by performing the items of "Create Account", "Query", and

"Transaction", where Fig. 6 is the TPS and Fig. 7 is TL. From the results, the TPS and TL keep stable for the "Query" and "Transaction", and increase slightly for the "Create Account". Therefore, the test environment has a minimal impact on the transaction performance, and the key management problem is the central aspect that can affect the efficiency of TPS and TL. An undeniable signature scheme with a small key size and high-security level can make the data-sharing process more efficient through BCCLS.

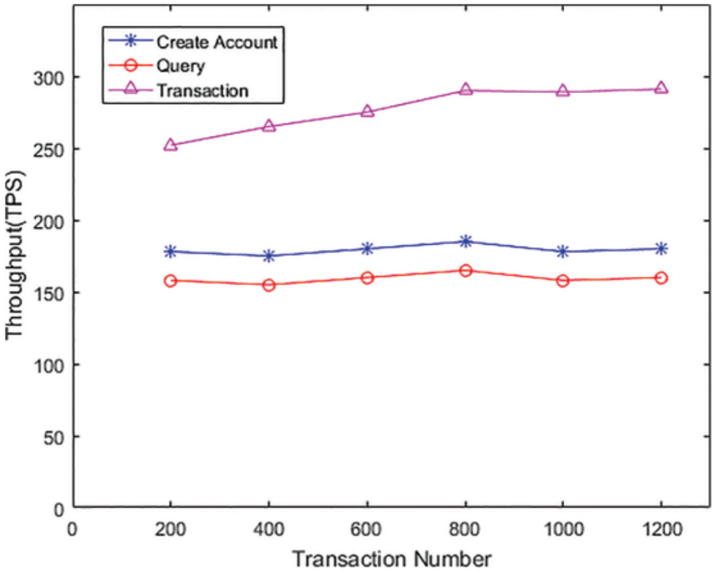

Figure 6: The transaction throughput (TPS)

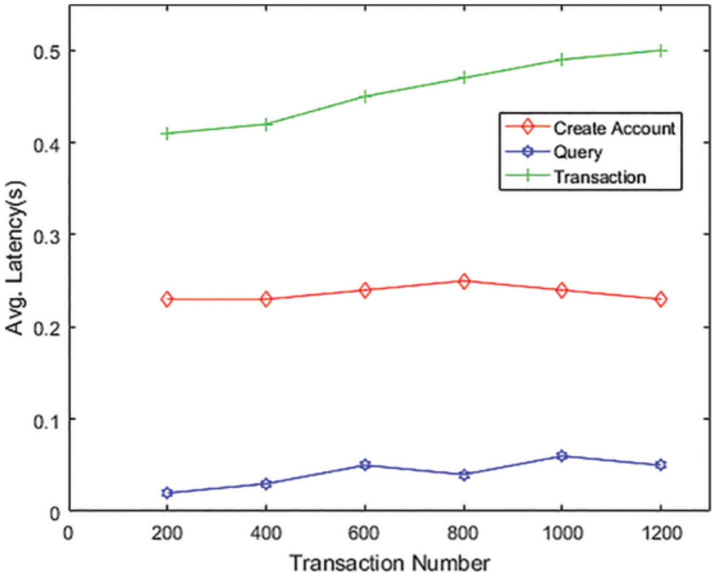

Figure 7: The average transaction latency (s)

Thirdly, the performance comparisons concerning TPS and TL between the Blockcoldchain [8], ColdBlocks [9], multi-mode blockchain [22], and the proposed BCCLS have been presented. The performance is executed by the same items of "Create Account", "Query", and "Transaction" with transaction number 1000, and the comparison results are shown in the following two figures Figs. 8 and 9. From the results, TPS of the three items in the proposed BCCLS is the highest than that in other systems, and TL of the three items is the lowest. These comparisons also show that the proposed BCCLS is more efficient than similar systems.

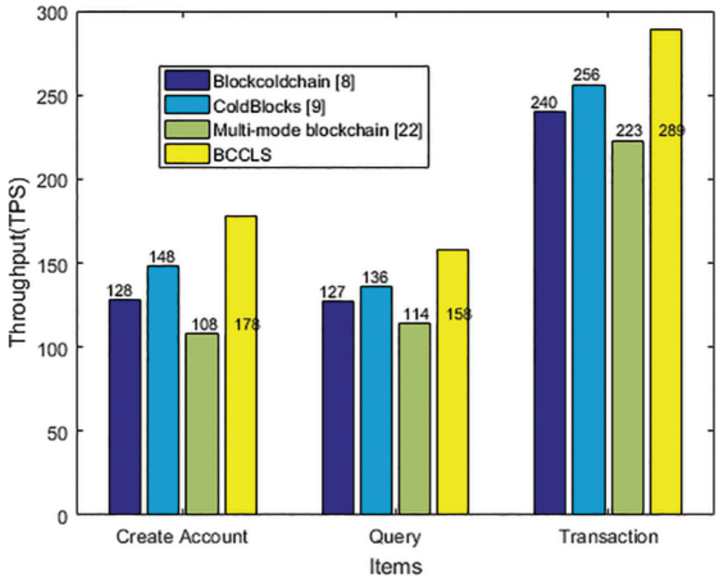

Figure 8: TPS comparison

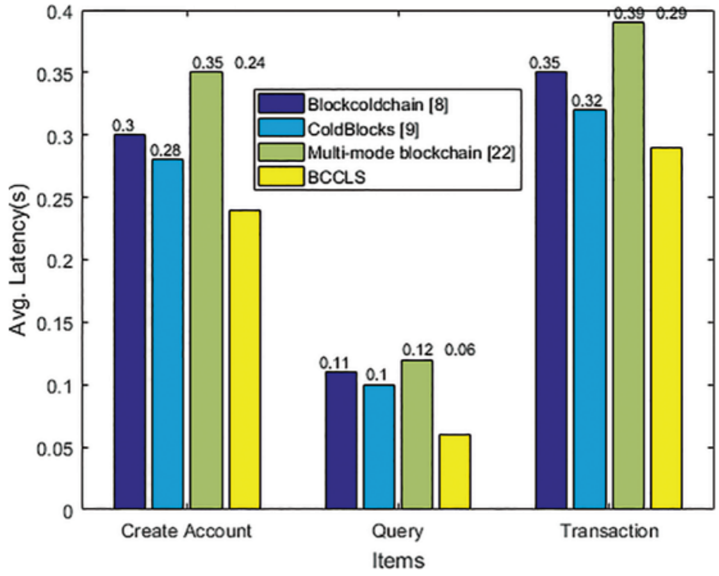

Figure 9: TL comparison

This paper provides a key size comparison of the proposed undeniable signature scheme and transaction process performance of the BCCLS. A cryptographic protocol is the security barrier of

BCCLS, and this undeniable signature scheme with a small key size can provide strong security for cold-chain logistics data sharing through BCCLS. Meanwhile, the performance evaluations of TSP and TL show the practicality and robustness of BCCLS, and the comparisons with other models also prove these results.

6 Conclusion

This paper focuses on data security and user privacy in traditional CCLS and introduces a BCCLS. This distributed platform can prevent data loss and tampering. It also can achieve secure data sharing through different cold-chain logistics parties. Then, security proof of the proposed undeniable signature scheme shows that it can guarantee logistics data security and user privacy. This scheme also has the property of anti-quantum attack security. In addition, the comparison results show that the proposed undeniable signature scheme is computationally efficient with more small key size than similar schemes. The performance evaluations show that TPS and TL keep stable with the transaction number increasing, which leads the transaction processing to a more efficient way by equipping a more efficient signature scheme. Therefore, the distributed BCCLS and undeniable signature scheme are secure, efficient, and practical, which have promising applications in the frozen food logistics data management.

In the future, the single-chain model is unsuitable for current blockchain-based CCLS, and multi-chain fusion is the development direction to focus on single-chain privacy and cross-chain scalability. For logistics data cross-chain sharing, the corresponding signature scheme is also needed for cross-chain transaction verification and identity authentication. There are still some other security issues, such as data encryption, key agreement, and fine-grained access control, which should be taken more consideration.

Funding Statement: This work was supported by the National Natural Science Foundation of China under Grant 92046001, 61962009, the Doctor Scientific Research Fund of Zhengzhou University of Light Industry under Grant 2021BSJJ033, Key Scientific Research Project of Colleges and Universities in Henan Province (CN) under Grant No.22A413010.

Conflicts of Interest: The authors declare they have no conflicts of interest to report regarding the present study.

References

[1] J. W. Han, M. Zuo, W. Y. Zhu, J. H. Zuo, E. L. Lü *et al.,* "A comprehensive review of cold chain logistics for fresh agricultural products: Current status, challenges, and future trends," *Trends in Food Science & Technology*, vol. 109, pp. 536–551, 2021.

[2] Z. Yu, Y. Liu, Q. Wang, L. Sun and S. Sun, "Research on food safety and security of cold chain logistics," *IOP Conference Series: Earth and Environmental Science*, vol. 647, no. 1, pp. 012176, 2021.

[3] A. Gorkhali and R. Chowdhury, "Blockchain and the evolving financial market: A literature review," *Journal of Industrial Integration and Management*, vol. 7, no. 1, pp. 47–81, 2022.

[4] C. Li, M. Dong, J. Li, G. Xu, X. Chen *et al.,* "Healthchain: Secure EMRs management and trading in distributed healthcare service system," *IEEE Internet of Things Journal*, vol. 8, no. 9, pp. 7192–7202, 2021.

[5] A. A. Khan, A. A. Wagan, A. A. Laghari, A. R. Gilal, I. A. Aziz *et al.,* "BIoMT: A state-of-the-art consortium serverless network architecture for healthcare system using blockchain smart contracts," *IEEE Access*, vol. 10, pp. 78887–78898, 2022.

[6] T. Li, W. Liu, A. Liu, M. Dong, K. Ota *et al.,* "BTS: A blockchain-based trust system to deter malicious data reporting in intelligent internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22327–22342, 2021.

[7] A. A. Khan, A. A. Laghari, T. R. Gadekallu, Z. A. Shaikh, A. R. Javed *et al.,* "A Drone-based data management and optimization using metaheuristic algorithms and blockchain smart contracts in a secure fog environment," *Computers and Electrical Engineering*, vol. 102, pp. 108234, 2022.

[8] R. D. Mendonça, O. S. Gomes, L. F. Vieira, M. A. Vieira, A. B. Vieira *et al.,* "Blockcoldchain: Vaccine cold chain blockchain, 2021. [Online]. Available: https://arXivpreprintarXiv:2104.14357

[9] K. N. Menon, K. Thomas, J. Thomas, D. J. Titus and D. James, "ColdBlocks: Quality assurance in cold chain networks using blockchain and IoT," in *Emerging Technologies in Data Mining and Information Security*, Singapore: Springer, pp. 781–789, 2021.

[10] J. Y. Wu and H. I. Hsiao, "Food quality and safety risk diagnosis in the food cold chain through failure mode and effect analysis," *Food Control*, vol. 120, pp. 107501, 2021.

[11] S. M. H. Bamakan, S. G. Moghaddam and S. D. Manshadi, "Blockchain-enabled pharmaceutical cold chain: Applications, key challenges, and future trends," *Journal of Cleaner Production*, vol. 302, pp. 127021, 2021.

[12] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.

[13] C. Li, M. Dong, J. Li, G. Xu, X. B. Chen *et al.,* "Efficient medical big data management with keyword-searchable encryption in healthchain," *IEEE System Journal*, vol. 15, no. 4, pp. 5521–5532, 2022.

[14] L. Wang, C. Huang and H. Cheng, "Quantum attack-resistant signature scheme from lattice cryptography for WFH," in *2021 IEEE 2nd Int. Conf. on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*, Nanchang, China, IEEE, pp. 868–871, 2021.

[15] K. Rajeshwaran and K. A. Kumar, "Cellular automata based hashing algorithm (CABHA) for strong cryptographic hash function," in *2019 IEEE Int. Conf. on Electrical, Computer and Communication Technologies (ICECCT)*, Coimbatore, India, IEEE, pp. 1–6, 2019.

[16] C. Balamurugan, K. Singh, G. Ganesan and M. Rajarajan, "Post-quantum and code-based cryptography—Some prospective research directions," *Cryptography*, vol. 5, no. 4, p. 38, 2021.

[17] C. Li, G. Xu, Y. Chen, H. Ahmad and J. Li, "A new anti-quantum proxy blind signature for blockchain-enabled internet of things," *CMC-Computers, Materials & Continua*, vol. 61, no. 2, pp. 711–726, 2019.

[18] C. Li, Y. Tian, X. B. Chen and J. Li, "An efficient anti-quantum lattice-based blind signature for blockchain-enabled systems," *Information Sciences*, vol. 546, pp. 253–264, 2021.

[19] Y. Cao, S. Xu, X. Chen, Y. He and S. Jiang, "A Forward-secure and efficient authentication protocol through lattice-based group signature in VANETs scenarios," *Computer Networks*, vol. 214, pp. 109149, 2022.

[20] S. Rawal, S. Padhye and D. He, "Lattice-based undeniable signature scheme," *Annals of Telecommunications*, vol. 77, no. 3, pp. 119–126, 2022.

[21] S. Kim, J. Kim and D. Kim, "Implementation of a blood cold chain system using blockchain technology," *Applied Sciences*, vol. 10, no. 9, pp. 3330, 2020.

[22] Y. Si, "Agricultural cold chain logistics mode based on multi-mode blockchain data model," *Computational Intelligence and Neuroscience*, vol. 2022, pp. 1–12, 2022.

[23] X. Hu, "Cold chain logistics model of agricultural products based on embedded system and blockchain," *Production Planning & Control*, vol. 33, pp. 1–12, 2022, [Online]. Available: https://doi.org/10.1080/09537287.2022.2101939

[24] J. Pan, N. Ye, H. Yu, T. Hong, S. Al-Rubaye *et al.,* "AI-Driven blind signature classification for IoT connectivity: A deep learning approach," *IEEE Transactions on Wireless Communications*, vol. 21, no. 8, pp. 6033–6047, 2022.

[25] J. Li, Y. Chen, J. Han, C. Liu, Y. Zhang *et al.,* "Decentralized attribute-based server-aid signature in the internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4573–4583, 2021.

[26] H. Huang, Y. Wu, F. Xiao and R. Malekian, “An efficient signature scheme based on mobile edge computing in the NDN-IoT environment,” *IEEE Transactions on Computational Social Systems*, vol. 8, no. 5, pp. 1108–1120, 2021.

[27] D. Zhang and T. Han, “Analysis of risk control factors of medical cold chain logistics based on ISM model,” in *2020 Chinese Control and Decision Conf. (CCDC)*, Hefei, China, IEEE, pp. 4222–4227, 2020.

[28] M. Ajtai, “Generating hard instances of lattice problems,” in *Proc. of the Twenty-Eighth Annual ACM Symp. on Theory of Computing*, Philadelphia PA, USA, pp. 99–108, 1996.

[29] V. Lyubashevsky, “Lattice signatures without trapdoors,” in *Annual Int. Conf. on the Theory and Applications of Cryptographic Techniques*, Springer, Berlin, Heidelberg, pp. 738–755, 2012.

[30] C. Aguilar-Melchor, S. Bettaieb, P. Gaborit and J. Schrek, “A code-based undeniable signature scheme,” in *IMA Int. Conf. on Cryptography and Coding*, Berlin, Heidelberg, Springer, pp. 99–119, 2013.