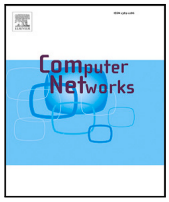
Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Computer Networks 224 (2023) 109595

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet



AQRS: Anti-quantum ring signature scheme for secure epidemic control with blockchain

Xue Chen [a,b,1,2], Shiyuan Xu [a,c,*,1,2], Yibo Cao [a,d,2], Yunhua He [a,e,*], Ke Xiao [a,*]

[a] School of Information Engineering, North China University of Technology, Beijing 100144, China
[b] Department of Computing, The Hong Kong Polytechnic University, Hung Hom, Hong Kong
[c] Department of Computer Science, The University of Hong Kong, Pokfulam, Hong Kong
[d] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
[e] Beijing Key Laboratory of Internet of Things Security, Institute of Information Engineering, Chinese Academy of Sciences (CAS), Beijing 100093, China

ARTICLE INFO

Keywords:
E-health
Lattice
Ring signature
Traceability
Linkability
Privacy protection
Blockchain

ABSTRACT

Epidemics, such as Corona Virus Disease 2019 (COVID-19), have serious consequences globally, of which the most effective way to control the infection is contact tracing. Nowadays, research related to privacy-preserving epidemic infection control has been conducted, nevertheless, current researchers do not regard the authenticity of records and infection facts as well as poor traceability. Moreover, with the emergence of quantum computing, there is a bottleneck in upholding privacy, security and efficiency. Our paper proposes a privacy-preserving epidemic infection control scheme through lattice-based linkable ring signature in blockchain, called AQRS. Firstly, our scheme adopts a blockchain with three ledgers to store information in a distributed manner, which offers transparency and immunity from the Single Point of Failure (SPoF) and Denial of Service (DoS) attacks. Moreover, we design a lattice-based linkable ring signature scheme to secure privacy-preserving of epidemic infection control. Significantly, we are the first to introduce the lattice-based linkable ring signature into privacy preserving in epidemic control scenario. Security analysis indicates that our scheme ensures unconditional users anonymity, record unforgeability, signature linkability, link non-slanderability and contact traceability. Finally, the comprehensive performance evaluation demonstrates that our scheme has an efficient time-consuming, storage consumption and system communication overhead and is practical for epidemic and future pandemic privacy-preserving.

1. Introduction

On January 30, 2020, COVID-19 caused by the "Severe Acute Respiratory Syndrome Coronavirus 2 (SARS-CoV-2)" virus, was announced a public health emergency of international concern [1]. With COVID-19 as an example, epidemics have the characteristics of often rapid transmission and powerful infectivity, which are extremely susceptible to mass mortality. According to the World Health Organization [2] and Johns Hopkins University [3], as of July, 2021, the number of COVID-19 infections in 188 countries and territories has reached 190 million, with more than 4 million deaths, posing a tremendous hazard to people's health and safety. Therefore, a robust epidemic infection control system is essential.

Those serious ramifications have forced most countries to implement extremely drastic measures [4,5] to prevent the spread of the epidemic, such as strongly urging people to reduce social activities and wear masks, imposing lockdowns on extremely infected metropolises such as Wuhan [6], and quarantining infected people [7]. Nevertheless, only isolating infected individuals is not effective in controlling the expansion of the epidemic. During the incubation period (14 days), patients do not show any symptoms of infection, but they are already contagious and can still interact with and transmit the virus to people. As early as the Black Death [8], contact tracing was considered the most effective measure to control outbreaks, with the aim of identifying people who may have been in contact with infected individuals and subsequently collecting further information on these contacts [9]. Thus, contact tracing is the most effective method to prevent and control outbreaks of epidemics (e.g. COVID-19).

It is necessary to protect the privacy of ordinary users from attacks while controlling infections. Privacy-preserving contact tracking systems have been proposed by some scholars to control infections

* Corresponding authors.
E-mail addresses: syxu666@connect.hku.hk (S. Xu), heyunhua@ncut.edu.cn (Y. He), xiaoke@ncut.edu.cn (K. Xiao).
[1] These authors contributed equally to this work.
[2] This work was finished when they were at the North China University of Technology.

https://doi.org/10.1016/j.comnet.2023.109595
Received 4 August 2022; Received in revised form 26 November 2022; Accepted 25 January 2023
Available online 28 January 2023

[10–12], however, these systems are based on centralized architectures, which may cause problems such as intermediate attacks, DoS attacks, and the SPoF. Blockchain technology has a tendency to be utilized widely in various scenarios [13,14], which is a public, distributed structure with conventional ones [15]. [16] adopts classical cryptography algorithm to achieve consensus without unforgeability, actually increases security requirements, such as security and privacy when connecting electric vehicles for charging [17]. Nowadays, some scholars apply blockchain technology to implement decentralized privacy-preserving epidemic infection control system [18]. The scheme proposed by Seham A. Alansari [19] implemented a decentralized privacy-preserving infection control system with COVID-19 and Zones' status ledgers on the blockchain. Nevertheless, in their scheme, keys are still centrally managed by the Key Distribution Center (KDC) and the aggregated signature applied in their system is not extremely secure and linkable. Digital signature can be used to protect and verify the authenticity so as to prevent forgery and tampering attacks, as well as to avoid repudiation and slander. Ring signatures with high anonymity and unforgeability, terminology was firstly formalized in [20]. In particular, a group of signers allow signing a message without the leakage of the anonymity of signatories, meaning that the ring signatures provide superior anonymity over group signatures [21]. Ring signature with linkability has been initially proposed in [22] as suitable for application to our scheme. Since epidemic outbreak control requires contact tracking, we demand linkability of different signatures of users. However, we also have to consider the quantum information [23] threat.

With the advent of quantum information and computation, more and more quantum computers and algorithms have been emerged [24,25], which led to severe threats to classical cryptography due to Elliptic Curve Digital Signature Algorithm [26], a mathematically difficult problem and the cornerstone of blockchain, could be threatened by Shor algorithm [27] that has the ability to calculate polynomial time mathematical factorization as well as discrete logarithmic decomposition. Some state-of-art researches indicated those computers through quantum information architecture is forthcoming [28]. Thus, post-quantum cryptography emerged [29], which is a novel branch of cryptologic research that dedicated to resident quantum computing attacks, and it mainly consists of four specific aspects, hash-based, code-based, multivariate-based and lattice-based cryptography [30]. To deal with such problems, lattice-based cryptography have been proposed not only to resist quantum computing attacks, but also more efficient and less consuming than other post-quantum cryptographies [31].

To address the above issues, we propose a privacy-preserving infection control scheme by designing a lattice-based linkable ring signature technique in post-quantum consortium blockchain networks. Our scheme employs three ledgers, the contents of which are shared by entities in the peer-to-peer network, using a consistent algorithm to agree on ledger contents, to record public access contact information, region infection level, classification and infected patients, user public key and anonymous credentials, respectively. Meanwhile, lattice-based linkable ring signature robustly maintains system security, user privacy as well as contact traceability. Its linkability allows one to detect, if necessary, whether two signatures are generated by the same signatory while still retaining their external anonymity. The signature is proven to be secure under the Small Integer Solution (SIS) assumption under the Random Oracle Model (ROM), with the capability to guarantee unconditional user anonymity, signature linkability, unforgeability, non-slanderability, and traceability. More critically, our scheme is resistant to quantum computing attacks and has strong system security while ensuring user privacy and infection control efficiency.

Our paper main contributions are as follows:

(1) We propose a privacy-preserving epidemic infection control scheme by designing a lattice-based linkable ring signature in blockchain, called AQRS scheme, which is the first epidemic infection control scheme capable of resisting quantum computing attacks and ensures robust traceability.

(2) Lattice-based linkable ring signature provides unconditional anonymity, unforgeability, linkability, and non-slanderability to our scheme. Unconditional anonymity ensures user privacy, unforgeability and non-slanderability guarantee the authenticity of the records and links, linkability enables our epidemic infection control scheme to be extremely traceable.

(3) Three-ledgers blockchain is deployed in our scheme to record user access/contact information, anonymous credentials and public keys, as well as infection status and regional ranking, which brings distributed storage and transparency.

(4) We conduct a comprehensive performance evaluation which shows that the time-consuming, storage consumption and communication overhead are as expected.

The outline of this paper is as follows: Section 2 covers the preliminary knowledge. Section 3 presents the system models, threat model and design goals. Our infection control scheme will be elaborated in Section 4, while the complete procedures and algorithms of our proposed signature will be shown in Section 5. The security analysis and experimental performance evaluation are in Sections 6 and 7, respectively. Section 8 gives the related work. At last, the conclusion of this paper is provided in Section 9.

2. Preliminaries

The main notations are shown in Table 1.

2.1. Fundamental knowledge

Definition 1 (*Lattice*). Let $A = [a_1, a_2, \dots, a_m] \in \mathbb{Z}_q^{n\times m}$ are m linearly independent vectors in n-dimensional space. Lattice L is composed of the linear combination of all integer coefficients of $a_1, a_2, \dots, a_n$, we can define: $L(A) = \{\sum_{i=1}^{n} x_i a_i : x_i \in \mathbb{Z}, i = 1, 2, \dots, n\}$, where $a_1, a_2, \dots, a_n$ is known as a basis of L. Given a prime q, a matrix $A \in \mathbb{Z}_q^{n\times m}$, we define: $L_q(A) = \{y \in \mathbb{Z}^m : y = A^T x \mod q, x \in \mathbb{Z}^n\}$ and $L_q^{\perp}(A) = \{y \in \mathbb{Z}^m : Ay = 0 \mod q\}$.

Definition 2 (*SIS Assumption*). Given an integer q, a matrix $A \in \mathbb{Z}_q^{n\times m}$, and a real constant $\beta \geq 0$, find a non-zero vector v, such that $Av \equiv 0 \mod q$ and $\|v\| \leq \beta$.

Definition 3 (*Statistical Distance*). Given random variables X, Y over a domain D, we define the Statistical Distance between X, Y: $\Delta(X, Y) = \frac{1}{2}\sum_{a\in D} |Pr[X = a] - Pr[Y = a]|$.

Definition 4 (*Discrete Gaussian Distribution*). Let $\rho_{c,\sigma}(x) = \exp\frac{-\pi\|x-c\|^2}{\sigma^2}$ be the standard Gaussian function which c represents the center and σ represents the standard deviation. Then we define the Discrete Gaussian Distribution over Lattice L as $D_{L,c,\sigma}(x) = \frac{\rho_{c,\sigma}(x)}{\rho_{c,\sigma}(L)}$.

Lemma 1 (*TrapGen [32]*). *Let $q \geq 2$, $m \geq 2n \log q$. There existing a polynomial time algorithm $TrapGen$, it outputs a matrix $A \in \mathbb{Z}_q^{n\times m}$ statistically close to uniform distribution and a trapdoor basis $Tr_A \in \mathbb{Z}^{m\times m}$, such that $\|Tr_A\| \leq O(n \log q)$ and $\|\widetilde{Tr_A}\| \leq O(\sqrt{n \log q})$.*

Lemma 2 (*SamplePre [32]*). *Given $L_q^{\perp}(A)$, a trapdoor base $Tr_A \in \mathbb{Z}^{m\times m}$, a parameter $s \geq \|\widetilde{Tr_A}\|\omega(\sqrt{\log m})$, and a vector $v \in \mathbb{Z}_q^n$. Then, the $SamplePre$ algorithm outputs a vector w statistically close to $D_{L_q^{\perp}(A),s}$, such that $Aw = v \mod q$.*

Lemma 3 (*Rejection Sampling [33]*). *Let $V = v \in \mathbb{Z}^m : \|v\| \leq t$, $\sigma = \omega(t\sqrt{\log m})$ and $h : V \to \mathbb{R}$ is a distribution making V maps to $\mathbb{R}$ (the set of real numbers), then there exists a constant M, such that the following*

Table 1
Notations.

Notation	Description
U_i^O, U_i^I, U_i^C, U_i^S	The i-th user, infected user, close contact user and sub-close contact user, respectively
$Cred_{U,c}^i$	The i-th anonymous credential of the user
$Score$	Score of user anonymous credentials
$T_{U,Cred}^i$	Timestamp of user anonymous credentials
ϑ_U^P, ϑ_I^{Posi}, ϑ_H^{Posi}, ϑ_{MH}^E	Signature of user access, infected user, hospital, and ministry of health
(pk_i, sk_i)	A pair of public key and secret key of i-th user
L	Lattice
X, Y and $\Delta(X,Y)$	Random variables and statistical distance
l	Ring member
$x \leftarrow S$	Uniformly random sample
Random oracle H	$\{0,1\}^*$
$\mathbb{R}^m$, $\mathbb{Z}^m$	The m-dimensional real and integer vector space
$\|x\|$	Euclidean parametrization of the vector x
$\mathbb{Z}_q^{n\times m}$	Module q residual class ring on $n \times m$ matrix space
D	The discrete gaussian distribution
$A = [a_1, a_2, \ldots, a_m]$	The m linearly independent vectors
$\widetilde{A}$	The matrix A after Gram–Schmidt orthogonalization
μ	Message
PKO, SKO, $SignO$	Oracle of pk_i, sk_i,and $\vartheta_L(\mu)$, respectively
$Pr[]$	The probability of the event occurring
$\rho_{c,\sigma}(x)$	Standard gaussian function
R	The matrix
q	The prime number
β, M	The real constant
Tr_A, Tr_B	The trapdoor base
$\mathbb{R}$	The set of real numbers
$v_1, v_2, \ldots, v_n$	The basis of $\mathbb{R}^n$
$\widetilde{v}$	The column vector during Gramm-Schmidt orthogonalization
$\mathcal{R}$	The ring $\mathbb{Z}[x]/f(x)$
$\mathcal{R}_q$	The quotient ring $\mathbb{Z}_q[x]/f(x)$

two cases output distributions which their statistical distance is not more than $\frac{2^{-\omega(\log m)}}{M}$ *:*

Case 1: Sample $v \leftarrow h$, $z \leftarrow D_{v,\sigma}^m$, *outputs* (z, v) *with probability* $min(\frac{D_\sigma^m(z)}{M D_{v,\sigma}^m(z)}, 1)$.

Case 2: Sample $v \leftarrow h$, $z \leftarrow D_\sigma^m$, *outputs* (z, v) *with probability* $\frac{1}{M}$. *Moreover, Case 1 has an output probability of at least* $\frac{1-2^{-\omega(\log\ m)}}{M}$.

Lemma 4 (*BasisDel [34]*)**.** *Set a positive integer* $m \geq 2n\ log\ q$, $q \geq 3$. *Given* $L_q^\perp(A)$ *and trapdoor base* $T_A \in \mathbb{Z}^{m\times m}$, *invertible matrix R is on* $\mathbb{Z}_q^{m\times m}$, $s \geq \|\widetilde{T_A}\| \cdot \sqrt{n\ log\ q} \cdot \omega(\sqrt{log\ m} \cdot \omega(log^{1.5}\ m))$. *The BasisDel algorithm outputs* $L_q^\perp(B)$ *and trapdoor basis* $T_B \in \mathbb{Z}^{m\times m}$ *responding to* $L_q^\perp(B)$, *where* $B = AR^{-1}\ mod\ q$. *In particular, when s takes the minimum value, we have* $\|\widetilde{T_B}\| \leq \|\widetilde{T_A}\| \cdot m^{1.5} \cdot \omega(log^2\ m)$.

Lemma 5 (*SampleDom [32]*)**.** *Set parameters n and* σ, *the algorithm SampleDom selects a random vector* $v \in \mathbb{Z}^m$ *according to the distribution* $D_{\mathbb{Z}^m,\sigma}$, *and satisfies* $\|v\| \leq \sigma\sqrt{m}$ *with a great probability.*

Definition 5 (*Gramm–Schmidt orthogonalization*)**.** Let $v_1, v_2, \ldots, v_n$ be a basis of $\mathbb{R}^n$, then set $\widetilde{v}$ to be the column vector during Gramm–Schmidt orthogonalization. Thus, the Gramm–Schmidt orthogonalization of $v_1, v_2, \ldots, v_n$ is: $\widetilde{v_1} = v_1$, $\widetilde{v_i} = v_i - \sum_{j=1}^{i-1} \frac{v_i \cdot \widetilde{v_j}}{\widetilde{v_j} \cdot \widetilde{v_j}} \widetilde{v_j} (i = 2, 3, \ldots, n)$.

2.2. Lattice-based linkable ring signature

In our scheme, the ring signature technique is utilized to realize the signature operation on the epidemic records. No centralized administrator in the ring signature and also no cooperation among ring members is required to generate the signature. It has strong anonymity and signature unforgeability, well suitable for the requirements of user privacy protection as well as authenticity and integrity of epidemic records in secure epidemic control scenarios. We propose the AQRS scheme, which is a ring signature with linkable property and is able to resist quantum computing attacks, to protect user privacy, ensuring the efficient epidemic tracking, with the following proposed design objectives.

(1) Enquiry Oracles

There are mainly three oracles in our proposed AQRS scheme, which can be queried by any adversaries depending on the type of security games.

(1) $pk_i \leftarrow PKO(\perp)$: The Public-Key Oracle is utilized to add new guests to our system. The input should be the identity of a ring user, such as their index i. That will return the Public-Key pk_i.

(2) $sk_i \leftarrow SKO(pk_i)$: The Secret-Key Oracle, after inputs one Public-Key pk_i according to PKO, it will returns the corresponding Secret-Key sk_i through $AQRS.KeyExt(p, s)$, showing in the AQRS algorithm.

(3) $\vartheta_L(\mu) \leftarrow SignO(w, L, pk_i, \mu)$: This oracle can be described as after inputs group size w, ring set L of w, Public-Key pk_i and a message $\mu \in \{0,1\}^*$, this oracle will return the valid Signature $\vartheta_L(\mu)$.

(2) Unconditional anonymity

It is infeasible to distinguish pk with $Prob = \frac{1}{2}$ for any efficient attacker. The anonymity of the linkable ring signature is characterized by the following $game_{anony}$ between efficient attacker A and challenger C.

(1) Initial phase: The challenger C generates key pair (pk_i, sk_i) and then sends pk_i to the efficient adversary A.

(2) Query phase: The efficient attacker A can access the PKO, SKO and $SignO$ oracles in Probabilistic Polynomial Times (PPT).

(3) Challenge phase: The efficient attacker A will give the challenger C two indices i_0, i_1 and a message $\mu \in \{0,1\}^*$. The challenger C chooses the b^C randomly in $\{0,1\}$ and signs on μ using the key pair pk_{i_b}, sk_{i_b} according to the $AQRS.SigExt$ algorithm.

(4) Guessing phase: Then the efficient attacker A will guess b^A. If $b^A = b^C$, the efficient attacker A wins the game. Finally, it generates the outcome

$$Output^{anony} = \begin{cases} 1, if\ b^A = b^C \\ 0, else \end{cases} \quad (1)$$

A wins the $game_{anony}$

$$iff \begin{cases} pk_0, sk_0 \ cannot \ used \ by \ SKO \ and \ SignO \\ The \ Output^{anony} = 1 \ with \ Prob = \frac{1}{2} \end{cases} \tag{2}$$

Thus, the probability of A wins the $game_{anony}$ is defined as: $Adv_A^{anony} = |Prob[b^A = b^C] - \frac{1}{2}|$.

Definition 6 (*Unconditional Anonymity*)**.** For any efficient attacker A, if Adv_A^{anony} is negligible, we say that AQRS scheme is unconditional anonymous.

(3) Unforgeability

The unforgeability of one linkable ring signature can describe as through the following $game_{unfo}$ between efficient attacker A and challenger C.

(1) Initial phase: The challenger C generates key pair (pk_i, sk_i) and then sends pk to the efficient adversary A.

(2) Query phase: The efficient adversary A accesses the PKO, SKO, $SignO$ oracles and inquires about the secret key sk_i.

(3) Forgery phase: The efficient adversary A forges a signature $\vartheta_L^*(\mu^*)$. The adversary wins if the forged signature is valid.

A will win the $game_{unfo}$

$$iff \begin{cases} AQRS.SigVeri(\vartheta_L(\mu)) =' Valid' \\ \forall pk \in L, pk \leftarrow PKO \\ \forall pk \in L, SKO \nleftarrow pk \\ \forall \vartheta_L^*(\mu^*) \ was \ not \ generated \ by \ SingO \ before \end{cases} \tag{3}$$

Therefore, we can denote that the probability of A wins the $game_{unfo}$ is: $Adv_A^{unfo} = Prob[A \quad wins \quad the \quad game_{unfo}]$.

Definition 7 (*Unforgeability*)**.** For an efficient adversary A, if Adv_A^{unfo} is negligible, we say that AQRS scheme is unforgeable.

(4) Linkability

It is feasible that if one efficient adversary link two signatures $\vartheta_L(\mu)$, $\vartheta'_{L'}(\mu')$ generated by same sk_π. The linkability of lattice-based linkable ring signature can describe through following $game_{linkability}$ between efficient attacker A and challenger C.

(1) Initial phase: The challenger C generates key pair (pk_i, sk_i) and then sends pk to the efficient adversary A.

(2) Query phase: The efficient adversary A has the ability to access the PKO, SKO, and $SignO$ Oracles within PPT and inquires about the secret key sk_i and signature $\vartheta_L(\mu)$.

(3) Challenge phase: The efficient adversary A gives two signatures $\vartheta_L(\mu)$ and $\vartheta'_{L'}(\mu')$ as well as the lists L and L', respectively.

(4) Guessing phase: After that, A will win the $game_{linkability}$

$$iff \begin{cases} AQRS.SigVeri(\vartheta_L(\mu)) =' Valid' \\ AQRS.SigVeri(\vartheta'_L(\mu')) =' Valid' \\ AQRS.SigLink(\vartheta_L(\mu), \vartheta'_L(\mu')) =' Unlink' \\ pk_L \leftarrow PKO, pk_{L'} \leftarrow PKO \\ sk_\pi \overset{only \ enquire \ once}{\longleftarrow} SKO(pk_\pi) \end{cases} \tag{4}$$

Definition 8 (*Linkability*)**.** For an efficient adversary A, we say that AQRS scheme is linkable if $Adv_A^{linkability}$ is negligible.

(5) Non-slanderability

It is infeasible for any efficient attacker A to link two valid signatures $\vartheta_L(\mu)$ and $\vartheta'_{L'}(\mu')$ generated by different sk, which in another words, one efficient adversary A has ability to frame one valid user by signing valid signature. By this, A produces another valid signature to link successfully using $AQRS.SigLink$ algorithm. We use another $game_{non-sland}$ completed by an efficient adversary A and a challenger C to describe this in AQRS scheme.

(1) Initial phase: The challenger C generates key pair (pk_i, sk_i) and then sends pk to the efficient adversary A.

(2) Query phase: The efficient adversary A is given the access to PKO, SKO, and $SignO$ and can adaptively query that.

(3) Challenge phase: Initially, $A \overset{L \ of \ pk}{\longleftarrow} C$, then, $A \overset{pk_\pi}{\longleftarrow} PKO(\perp)$ and $A \overset{sk_\pi}{\longleftarrow} SKO(pk_\pi)$. After that, C utilizes $\vartheta_L(\mu) \overset{SignO(sk_\pi)}{\longleftarrow} C$ to give $\vartheta_L(\mu)$ to A. Finally, it processes $\vartheta'_L \overset{SignO(w-1)}{\longleftarrow} A$.

(4) Guessing phase: Adversary A wins the $game_{non-sland}$

$$iff \begin{cases} Valid \overset{AQRS.SigLink}{\longleftarrow} \vartheta_L(\mu) \\ Valid \overset{AQRS.SigLink}{\longleftarrow} \vartheta'_L(\mu) \\ \vartheta'_L \nleftarrow (pk_\pi, sk_\pi) \\ Linked \overset{AQRS.SigLink}{\longleftarrow} (\vartheta_L(\mu), \vartheta'_L(\mu)) \end{cases} \tag{5}$$

In this way, the advantage of the non-slanderability in the lattice-based linkable ring signature can describe as: $Adv_A^{non-sland} = Prob[A \ wins \ the \ game_{non-sland}]$.

Definition 9 (*Non-slanderability*)**.** For one efficient attacker A, we say that AQRS scheme is non-slanderable if $Adv_A^{non-slanderability}$ is negligible.

2.3. Blockchain

In 2008, Satoshi Nakamoto proposed the concept of blockchain [15, 35], which is a distributed database managed autonomously through peer-to-peer Network and distributed servers. In blockchain network, all data are decentralized stored in nodes involved in recording data and maintained by all participants rather than stored centrally in the central node, which is a secure, unforgeable, and trustworthy distributed database.

The blockchain possesses numerous outstanding properties, such as decentralization, transparency and traceable transactions, etc. In the blockchain network, there are no centralized nodes and no need to trust each other to perform transactions. In addition, as long as less than 50% of the nodes are failed and deactivated, all of them can carry out normal work and there will be no system collapse. The operation rules of the blockchain and its data information are open and transparent, and each transaction cannot be modified or deleted after it is uploaded to the blockchain. All the nodes in the blockchain are anonymous and are authenticated by a specific verification method. The proper operation of the blockchain and its trustworthiness is hampered when and only when more than 51% of the nodes are controlled by malicious users, which is almost impossible.

The aforementioned properties provide our scheme with record transparency and immunity to attacks such as SPoF and DoS, which strongly guarantee the security and effectiveness of the epidemic infection control system.

3. System model, threat models and design goals

3.1. System model

Our scheme consists of eight entities, including Users, Infected Users, Close Contacts, Sub-close Contacts, Public places, Identity and Key Generator (IKG), Ministry of Health (MH) and Hospitals. Specifically, user refers to healthy users. Infected user refers to users who is confirmed to be positive for nucleic acid by hospitals. Close contacts are people who have lived, worked, or contacted infected users within 14 days. Sub-close contacts are close contacts of close contacts. Public places are places where users have activities, such as shopping malls, parks, hotels, etc. The distribution and updating of user anonymous

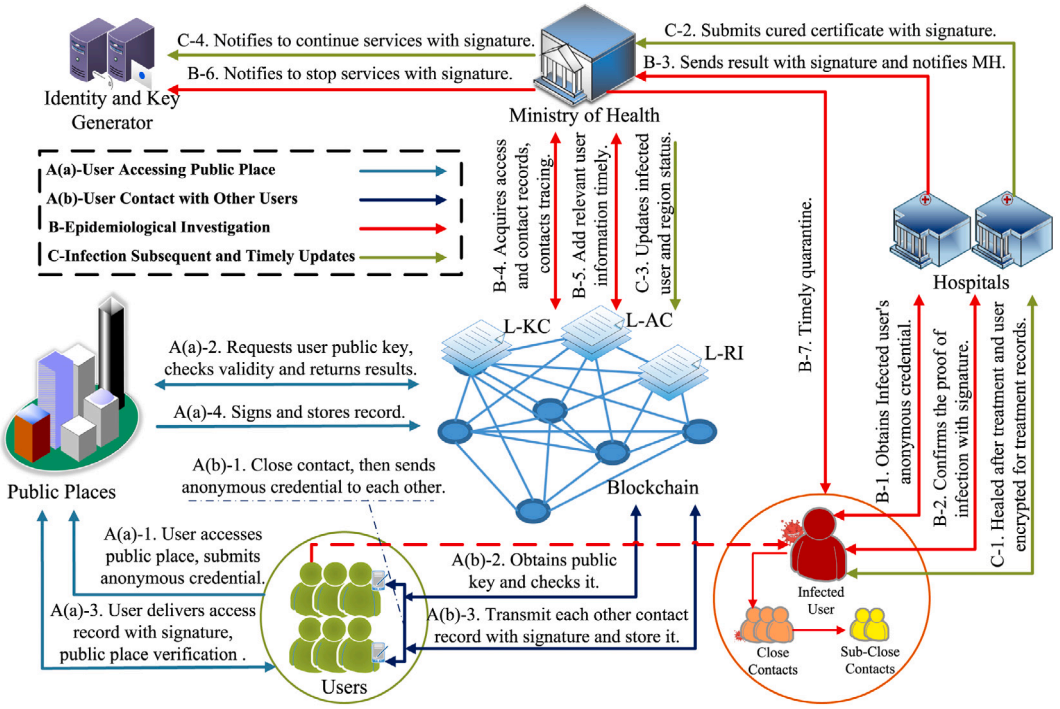


Fig. 1. System architecture diagram.

credentials and keys are the domain of Identity and Key Generator. Ministry of Health is responsible for identifying and uploading infected users to the blockchain, and notifying IKG to stop serving infected users until they are healed. Timely updates on infection levels in the regions and the release of information on infected users and their movements to alert the public are also the responsibility of MH. Hospitals offer users nucleic acid testing to confirm their infection with virus and treatment. Besides, three blockchain ledgers are set up to record ledger of public access contact information (L-AC), ledger of region infection level classification and infected patients (L-RI), ledger of user public key and anonymous credentials (L-KC), respectively.

3.2. Threat models

(1) Real identity recognition

During the epidemic control period, we require user to upload records when he/she accesses public places or comes into contact with other users. However, a malicious user may try to identify user's real identity information so as to guess whether this user is infected with epidemic or announce his/her daily movement habits and routes.

(2) Maliciously tampering or falsifying records

User access/contact records uploaded by users may be tampered with or falsified by adversaries, resulting in incomplete or inauthentic access records.

(3) Misreporting of infected individuals or close contacts

Ministry of Health release information on the movement trajectory of the infected individual within the latest 14 days to alert the public in a timely manner. However, if a healthy user is mistakenly reported as an infected person, his/her personal privacy information will be leaked wholly, which has severe consequences for his/her privacy.

(4) Insufficient tracking

Inadequate national tracking of infected patients and their close contacts can lead to a situation where infected users remain in widespread contact with healthy users, creating a greater likelihood of infection leading to uncontrolled infection.

(5) Quantum computing attacks

Epidemic outbreak prevention and control tracking also confront privacy and security issues under quantum computing attacks, which become a significant obstacle for outbreak prevention, control and tracking of infected individuals.

3.3. Design goals

(1) Decentralization and authentication transparency

Our scheme is based on a decentralized architecture with intense security. The trajectory of the infected individual's movements is transparent to the public, thus making tracking more effective, reassuring the public, and preventing social panic and speculation.

(2) Health user unconditional anonymity

In order to control infections and protect user privacy, we record information about users' access to public places and contacts while maintaining their anonymity.

(3) Record integrity and authenticity

Records including locality and time may be extremely disruptive to track if they are tampered with or falsified by malicious users. Therefore, we require to maintain integrity and authenticity of the records.

(4) Correct tracking of infected individuals

We require linkability and unforgeability of the user's signature and non-slanderability of the links to prevent misreporting of infections for a correct infection control scheme with traceability.

(5) Resisting quantum computing attacks

Our scheme requires the ability to resist quantum computing attacks in order to realize a upper level of security.

4. Our proposed privacy-preserving epidemic infection control scheme

4.1. Overview

As shown in Fig. 1, our scheme is constituted by 4 phases, including system initialization, user accessing public places or close contact with

other user, epidemiological investigation and infection subsequent and timely updates. Among them, the specific ring signature algorithm involved in Fig. 1 is described in Section 5 in detail. A full performance evaluation of the ring signature algorithm we employed and the epidemic infection control scheme we proposed are presented in Section 7 below.

The system initialization phase contains the registration of entities, the acquisition of key pairs and anonymous certificates. At the phase of user accessing public places or close contact with other users, if user wishes to access a public place, he/she needs to submit record to public place with signature, which will be verified as well as stored in the blockchain for subsequent tracking. When two users are in close contact, they are required to exchange and document contact record with each other via Bluetooth technology and store it on blockchain for subsequent epidemiological investigation. During epidemiological investigation phase the MH tracks infected individuals, including people contacted and places accessed in the last 14 days, etc. After completed tracing, the infected information is released to public and stored on the blockchain, which timely update of the status of users and areas are beneficial to social stability. Infection subsequent and timely updates phase is the follow-up phase of the epidemiological investigation, where the hospital is responsible for the treatment of infected users and notifies MH to update infected users and regional level status promptly.

4.2. System initialization

The system security parameter λ is set during initialization, and the public parameter pair (P, R) is obtained through Algorithm 2 in Section 5 as input to Algorithm 3 to obtain the key pair. Users obtain their temporary key pair (pk_i, sk_i) and anonymous credential $Cred^i_{U,c}$ from IKG. Hospitals, MH, and public places also obtain key pairs (pk_H, sk_H), (pk_{MH}, sk_{MH}), and (pk_P, sk_P), respectively, from the IKG. Note that both user's key pair (pk_i, sk_i) and the anonymous credential $Cred^i_{U,c}$ are temporary and valid only for a specified time period and updated frequently. In addition, the lattice-based linkability ring signature is applied to all signature segments in our epidemic infection control scheme, where Section 5 details the procedures for generating, verifying and linking signatures.

4.3. User accessing public places or close contact with other users

4.3.1. User accessing public places

As shown in Fig. 2, when one user U_i wishes to access a public place, he/she is required to submit an anonymous credential $Cred^i_{U,c}$ to the public place in order to authenticate while remaining anonymous. Due to the unconditional anonymity of AQRS scheme, the actual identities of users are hidden to prevent a privacy breach. When the public place receives it, it is necessary to obtain its public key pk_i from L-KC and verifies it according to Algorithm 1. The time complexity of Algorithm 1 is $O(1)$.

If one user is allowed to enter, he/she should send entry time, exit time, location information and sign the information through Algorithm 4 in Section 5 with his/her secret key as $R^i_A = [Time(T_{entry}, T_{exit}), Location, \vartheta^P_U]$ so as to safeguard user privacy. Meanwhile, the unforgeability and non-slanderability of the AQRS scheme assure the integrity and authenticity of the record.

Public place receives and confirms the correctness of record and validity of signature through Algorithm 5 in Section 5. If it is $'valid'$, public place will sign the record with its secret key and stores it on L-AC, otherwise, it will ask the user to send record again. If one user refuses to cooperate, public place has the responsibility to notify MH to take appropriate measures.

Algorithm 1 Check (A or RN or RU)

Input: Public place Signature ϑ^i_P, User credential $Cred^i_{U,c}$, Timestamp $T^i_{U,Cred}$
Output: Accept A, or Reject and Notify RN, or Reject and Update RU

```
if c = green then
    Cred^i_{U,c} = 2
end if
if c = yellow then
    Cred^i_{U,c} = 1
end if
if c = red then
    Cred^i_{U,c} = -1
end if
if T^i_{U,Cred} is valid then
    T^i_{U,Cred} = 1
else
    T^i_{U,Cred} = 0
end if
SET Score = Cred^i_{U,c} · T^i_{U,Cred}
if Score = 1 or -1 then
    Return RN
end if
if Score = 0 then
    Return RU
end if
if Score > 1 then
    Return A
end if
```

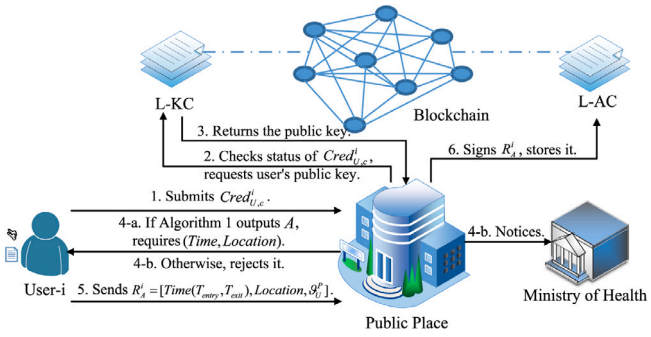


Fig. 2. User accesses public place.

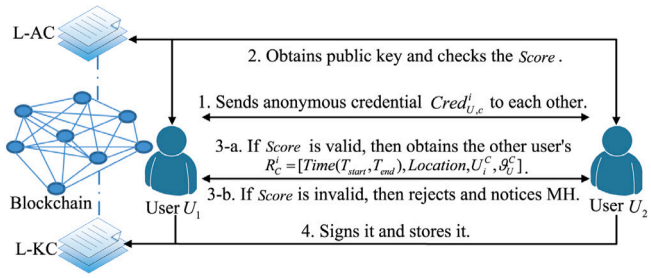


Fig. 3. Direct and close contact between two users.

4.3.2. One user close contact with other users

The reason why we concerned about two users coming into close contact is that the risk of infection is extremely high. If user U_1 and user U_2 are in close contact, they will be required to examine each other's status and record it via Bluetooth smartphone before contact.

The flow of user contact is shown in Fig. 3. U_1 and U_2 initially need to transmit their anonymous credentials to each other and sign them through Algorithm 4 to ensure that this anonymous status is delivered by the user himself/herself and to confirm the authenticity of the contact history mutually. They receive the partner's anonymous credentials and get their public keys through L-KC to verify them by Algorithm 5 and check their $Score$ of anonymous credential through Algorithm 1.

Having completed the above verification process, user U_1 and user U_2 submit to each other the contact records as $R^i_C = [Time(T_{Start}, T_{end}), Location, U^C_i, \vartheta^C_U]$ of their contact with a signature of Algorithm 4 to confirm that it is signed by the user and this recorded information cannot be tampered. After they received the signed records from each other, they will deposit them on L-AC.

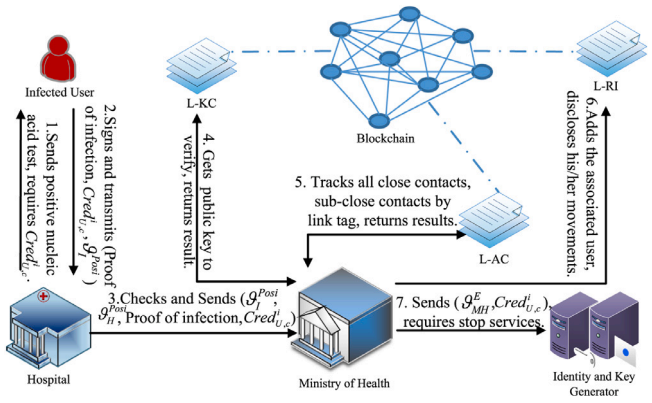


Fig. 4. Epidemiological investigation process.

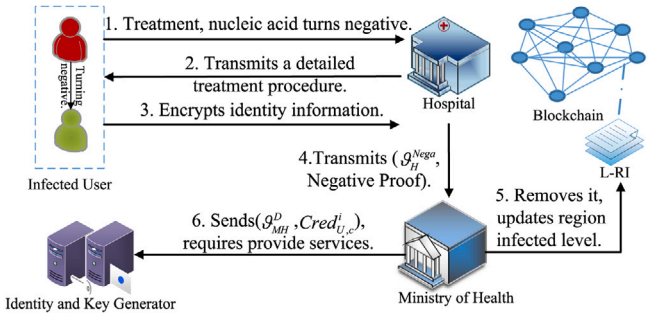


Fig. 5. Infection subsequent and timely updates.

4.4. Epidemiological investigation

Tracing is the most competent approach to control epidemic outbreaks. In general, infected users are our primary targets for epidemiological follow-up. Close contacts and sub-close contacts should be isolated in designated infrastructures and at home respectively to prevent the spread of the epidemic (e.g. COVID-19) if they carry the virus or they are in the incubation period and transmit it to healthy users.

Epidemiological tracing process is shown specifically in Fig. 4. If a user tests positive for nucleic acid, he/she will be confirmed as infected. The hospital firstly obtains $Cred^i_{U,c}$ from User U^O_i and signs the result by Algorithm 4 to confirm the identity of the infected user and the authenticity of the infection fact. User U^O_i then signs the result via Algorithm 4 to ensure that it has been approved by the user, as action routes of infected user are released to the community to secure the safety of people's lives. Two-way signatures for hospitals and users prevent efficient attackers from falsifying social panic and false alarm attacks caused by infected users. The hospital transmits its signature ϑ^{Posi}_H, infected user signature ϑ^{Posi}_I, infected user's anonymous credentials $Cred^i_{U,c}$ and positive nucleic acid certificate to the MH to inform the subsequent steps.

Having received the notification from hospital, MH will obtain the user and hospital public key pk_i, pk_H from L-KC for verification adopt Algorithm 5. If it outputs $'valid'$, the user's $Cred^i_{U,c}$ with MH's confirmed signature will be sent to the IKG, which is requested to red mark the user's $Cred^i_{U,c}$ and stop providing services, such as updating the anonymous credential and key pair. Upon receipt of the request, IKG will verify the signature ϑ^E_{MH} of the MH via Algorithm 5, and perform the requirements of MH.

Tracking close and sub-close contacts of an infected user after he/she has been quarantined is principal for outbreak control. MH will derive all linked signatures of the infected user in 14 days from L-AC by the linkability of the lattice-based linkable ring signature, the exact steps is shown in Algorithm 6, which outputs $'Linked'$ if two signatures are signed by the same user. After that, MH searches all close and sub-close contacts by all signatures of infected user.

To control outbreak, the MH will convey all close contacts to designated sites for isolation and nucleic acid testing for 14 days, and all sub-close contacts will be isolated at home for 14 days. In addition, all users who have accessed the same locality at the same time can be identified through L-AC and should be notified by MH to self-monitoring their health status. IKG promptly revises the anonymous credentials status of all infected users, close contacts and sub-close contacts and MH adds them to L-RI. To ensure the safety of people's lives and the transparency of epidemic control, MH releases the movement of infected users to the community timely for public self-examination.

L-BC is also used to classify areas according to infected user situations in each region. There are three levels: high, medium, and low risk areas. The public can take different precautionary measures depending on the region level.

4.5. Infection subsequent and timely updates

The subsequent process of tracking the infected user is shown in Fig. 5. After the user's infection is confirmed, he/she should be referred by MH to the hospital, which is responsible for diagnosis and treatment. After an infected user's nucleic acid has turned negative, the identifying information for the detailed treatment record should be encrypted by the user. The hospital signs the result and transmits it to MH.

After verification via Algorithm 5 by MH, the user will be removed from the L-RI and announced to community that he/she had been cured. Then, IKG continues to provide serves and change his/her anonymous credentials to green.

5. Our designed lattice-based linkable ring signature

We demonstrate the specific procedures for lattice-based linkable ring signature, which is applied in Section 4.

5.1. $AQRS.Setup\ (P, R)$

The whole process has been described in Algorithm 2, which has the time complexity of $O(m)$. In our algorithms, $\mathcal{R}$ is the ring $\mathbb{Z}[x]/f(x)$, and $\mathcal{R}_q$ is denoted as the quotient ring $\mathbb{Z}_q[x]/f(x)$.

Algorithm 2 AQRS.Setup-Public Parameters (P,R)

Input: Security Parameter λ
Output: A pair of public parameter (P,R)

Set $(p_1, p_2, \cdots, p_{m-1}) \leftarrow \mathcal{R}_q^{1\times(m-1)}$
Set $(r_1, r_2, \cdots, r_{m-1}) \leftarrow \mathcal{R}_q^{1\times(m-1)}$
Let $P = (p_1, p_2, \cdots, p_{m-1})$
Let $R = (r_1, r_2, \cdots, r_{m-1})$
Return (P,R)

5.2. $AQRS.KeyExt\ (p, s)$

In this step, we have the public parameter $P = (p_1, p_2, \ldots, p_{m-1})$ and a key pair generated in ring $\mathcal{R}_q^{1\times(m-1)}$. We let $s^T = (s_1, s_2, \ldots, s_{m-1})$ belonging to $\mathcal{R}_q^{1\times(m-1)}$ and compute $p = P \cdot s \mod q$, which p is public-key and s is secret-key. The specific steps are described in Algorithm 3, with the time complexity of $O(m)$.

Algorithm 3 AQRS.KeyExt-key Pair (p,s)

Input: Public Parameter P
Output: Key Pair (p,s)

Use AQRS.KeyExt(P) ▷ $P \in \mathcal{R}_q^{1\times(m-1)}$
  Set $(s_1, s_2, \cdots, s_{m-1}) \in \mathcal{R}_q^{1\times(m-1)}$
  Let $s^T = (s_1, s_2, \cdots, s_{m-1})$
  Calculate $p = P \cdot s \mod q \in \mathcal{R}_q$ ▷ p is public-key and s is secret-key.
  Return (p, s)

5.3. AQRS.SigExt ($\vartheta_L(\mu)$)

After input the secret key s_π, message μ, public parameters $R = (r_1, r_2, \ldots, r_{m-1})$ as well as L which notes as a list of public keys, this algorithm will output a valid signature $\vartheta_L(\mu)$. Formal description of this algorithm is shown in Algorithm 4 and the time complexity is $O(lm)$.

Algorithm 4 AQRS.SigExt-Signature $\vartheta_L(\mu)$

Input: Secret-key s_π, message μ, list of public keys $L = (p_1, p_2, \cdots, p_l)$ and public parameters R and P
Output: Signature $\vartheta_L(\mu) = (c_1, t_1, t_2, \cdots, t_l, R, P)$

Use AQRS.SigExt (s_π, μ, L, R, P) ▷ π is a user number which $\pi \in \{1, 2, \cdots, l\}$
  Let $(2 \cdot R, -2 \cdot r + q) \in \mathcal{R}_{2q}^{l\times m}$ ▷ $r = R \cdot s_\pi \in \mathcal{R}_q$
  Let $R_{2q} = (2 \cdot R, -2 \cdot r + q)$
  Compute $(2 \cdot P, -2 \cdot p_\pi + q) \in \mathcal{R}_{2q}^{1\times m}$
  Let $P_{2q} = (2 \cdot P, -2 \cdot p_\pi + q)$
  Let $u = (u_1, u_2, \cdots, u_m)^T$ ▷ $u_i \leftarrow D_\vartheta^n$
  Compute $c_{\pi+1} = (R,\ L,\ R_{2q},\ \mu,\ P_{2q,\pi} \cdot \mu,\ R_{2q} \cdot \mu)$
for $(i = \pi+1, \pi+2, \cdots, l, 1, 2, \cdots, \pi-2, \pi-1)$ **do**
  Compute $(2 \cdot P, -2 \cdot p_i + q) \in \mathcal{R}_{2q}^{1\times m}$
  Let $P_{2q,i} = (2 \cdot P, -2 \cdot p_i + q)$
  Let $t_i = (t_{i,1}, t_{i,2}, \cdots, t_{i,m})^T$ ▷ $t_{i,j} \leftarrow D_\vartheta$
  Compute $c_{i+1} = (R, L, R_{2q}, \mu, P_{2q,i} \cdot t_i + q \cdot c_i, R_{2q} \cdot t_i + q \cdot c_i)$
end for
  Select b from {0,1} randomly ▷ b is a parameter
  Compute $t_\pi = u + s_{2q,\pi} \cdot c_\pi \cdot (-1)^b$
  Continue with $Prob(min\frac{D_\vartheta^{m+1}(t_\pi)}{M \cdot D_{s_{2q,\pi} \cdot c_{\pi,\vartheta}}^{m+1}(t_\pi)}, 1)$
Otherwise Restart
  Return Signature $\vartheta_L(\mu) = (c_1, t_1, t_2, \cdots, t_l, R, P)$

5.4. AQRS.SigVeri (Valid or Invalid)

This algorithm receives signature $\vartheta_L(\mu)$, message μ, list of public-keys L and public parameters $R = (r_1, r_2, \ldots, r_{m-1})$ as well as $P = (p_1, p_2, \ldots, p_{m-1})$. Its output is a decisional answer: Valid or Invalid. More details has been characterized in Algorithm 5. The time complexity is $O(wm)$.

Theorem 1. *According to the Lemma 4.4 in [33], we know that the bound on Euclidean norm $B = \eta\vartheta\sqrt{nm}$, $\forall\eta \geq 1$, $Prob[\|t_i\|_2 \geq \eta\vartheta\sqrt{nm}] \geq 1 - 2^{-\lambda}$. Moreover, the bound on infinity norm $\|t_i\|_\infty \leq \frac{q}{4}$ has been considered simultaneously. Thus, with obtained the signature $\vartheta_L(\mu)$ as for input, the output of Algorithm 5 is valid with probability of $1 - 2^{-\lambda}$.*

5.5. AQRS.SigLink (Linked or Unlinked)

We have illustrated this part in Algorithm 6, which has two valid signatures to input: $\vartheta_L(\mu_1) = (c_{1,\mu_1}, t_{1,\mu_1}, t_{2,\mu_1}, \ldots, t_{l,\mu_1}, r_{\mu_1})$ and $\vartheta_L(\mu_2) = (c_{1,\mu_2}, t_{1,\mu_2}, t_{2,\mu_2}, \cdots, t_{l,\mu_2}, r_{\mu_2})$. Having utilized Algorithm 6, we obtain $(r_{\mu_1} r_{\mu_2})$, which is a linkability tag between two signatures. It turns out two signatures have been linked if $r_{\mu_1} = r_{\mu_2}$. The time complexity of Algorithm 6 is $O(1)$.

Algorithm 5 AQRS.SigVeri-Signature Verification (Valid or Invalid)

Input: Signature $\vartheta_L(\mu) = (c_1, t_1, t_2, \cdots, t_l, r)$, list of public keys $L = (p_1, p_2, \cdots, p_l)$, message μ and public parameters R and P
Output: Valid or Invalid

Use AQRS.SigVeri $(\vartheta_L(\mu), R, P)$
if $R_{2q} = (2 \cdot R, -2 \cdot r + q) \in \mathcal{R}_{2q}^{l\times m}$ **then**
  for $(i = 1, 2, \cdots, w)$ **do**
    Compute $(2 \cdot P, -2 \cdot p_i + q) \in \mathcal{R}_{2q}^{l\times m}$
    Let $P_{2q,i} = (2 \cdot P, -2 \cdot p_i + q)$
    if $c_{i+1} = R_1(L, R_{2q}, \mu, P_{2q,i} \cdot t_i + q \cdot c_i, R_{2q} \cdot t_i + q \cdot c_i)$ **then**
      Continue
    end if
    if $\|t_i\|_\infty \leq \frac{q}{4}$ ▷ $\frac{q}{4}$ is based on infinity norm [33] **then**
      Continue
    end if
  end for
end if
if $c_1 = R_1(L, R_{2q}, \mu, P_{2q,l} \cdot t_l + q \cdot c_l, R_{2q} \cdot t_l + q \cdot c_l)$ **then**
  Return Valid
else
  Return Invalid
end if

Algorithm 6 AQRS.SigLink-Signature Linkability (Linked or Unlinked)

Input: Signature $\vartheta_L(\mu_1)$ and Signature $\vartheta_L(\mu_2)$
Output: Signature Linkability (Linked or Unlinked)

Use AQRS.SigLink $(\vartheta_L(\mu_1), \vartheta_L(\mu_2))$
if (AQRS.SigVeri($\vartheta_L(\mu_1)$)=Valid AND AQRS.SigVeri($\vartheta_L(\mu_2)$)=Valid) **then**
  if $r_{\mu_1} = r_{\mu_2}$ ▷ r_{μ_1} and r_{μ_2} are the linkability tags of $\vartheta_L(\mu_1)$ and $\vartheta_L(\mu_2)$, respectively **then**
    Return Linked
  end if
else
  Return Unlinked
end if

6. Security analysis

6.1. Correctness

Theorem 2. *Our AQRS.SigExt algorithm guarantees that signature $\vartheta_L(\mu)$ signed by honest signatories are valid with preponderant probabilities.*

Proof. According to the input of *AQRS.SigVeri*, we have to say that the output of it should be consider to accept after acquired its input $(\mu, L, \vartheta_L(\mu))$ under the condition of $\vartheta_L(\mu_1) = (c_1, t_1, t_2, \ldots, t_l, r)$ is the output of *AQRS.SigExt* algorithm. Thus, we have to prove that during the step of compute $R_1(L, R_{2q,\mu}, P_{2q,i} \cdot t_i + q \cdot c_i + R_{2q} \cdot t_i + q \cdot c_i)$, the result is equivalent to c_1.

During the steps of *AQRS.SigExt* algorithm, we set $c_{i+1} = R_1(L, R_{2q,\mu}, P_{2q,i} \cdot t_i + q \cdot c_i, R_{2q} \cdot t_i + q \cdot c_i)$ and c_{i+1} in the *AQRS.SigVeri* algorithm is same as the former one due to the fact that

$$iff \begin{cases} P_{2q,i} \cdot t_i + q \cdot c_i(AQRS.SigExt) \\ \triangleq P_{2q,i} \cdot t_i + q \cdot c_i(AQRS.SigVeri) \\ R_{2q} \cdot t_i + q \cdot c_i(AQRS.SigExt) \\ \triangleq R_{2q} \cdot t_i + q \cdot c_i(AQRS.SigVeri) \end{cases} \tag{6}$$

Theorem 3. *Our AQRS.SigLink algorithm will output Linked with overwhelming probability after obtaining two signatures ϑ_{μ_1} and ϑ_{μ_2} of message μ_1 and μ_2 by a valid user π together with the public-keys' list L.*

Proof. Having obtained two valid signature $\vartheta_L(\mu_1)$ and $\vartheta_L(\mu_2)$ and verified by the $AQRS.SigVeri$ algorithm accurately, we have to prove that two tags of achievement of linkability r_{μ_1} and r_{μ_2} has to be equivalent. Thus, the proof can convert into prove $R_{2q,\mu_1} = R_{2q,\mu_2}$, which is shown as follows: $R_{2q,\mu_1} = (2 \cdot R, -2 \cdot r_{\mu_1} + q)$, $R_{2q,\mu_2} = (2 \cdot R, -2 \cdot r_{\mu_2} + q)$, where R means public-parameter and $r_{\mu_1} = r_{\mu_2} = R \cdot r_\pi + q$.

To begin with, we know $Prob[2R - 2R = 0] = 1$. Then, we also have $Prob[-2 \cdot r_{\mu_1} + q = 2 \cdot r_{\mu_2} + q] = 1$ due to the fact that they both utilize the secret-key s_π of the user.

Correctness underpins our epidemic infection control scheme, ensuring that users signature is accurate.

6.2. Unforgeability

Theorem 4. *Our AQRS scheme satisfies unforgeability for any efficient PPT adversary A, which can reduce to the SIS assumption.*

Proof. We assume that the efficient attacker A can successfully forge the signature with a non-negligible probability p and we will show how the challenger C find a vector e using forgery signature of efficient attacker A, where e is a solution of the SIS problem.

The game process is as follows:

(1) Setup: Given $q \le 3$, $m \ge 5$ λ log q, $L = (O\sqrt{\lambda \ log \ q})$, $\vartheta = L(\omega\sqrt{log \ \lambda})$, we input security parameter λ, and make two operations: ① For $1 \le i \le l$, C calls $TrapGen$ to output $P_i \in \mathbb{Z}_q^{n\times m}$ obeying a randomly distribution and a set of bases T_i of the lattice $L^\perp(P_i)$, such that $\|\widetilde{T_i}\| \le L$. Then, C selects two hash functions: $R_1 : \{0,1\}^* \to \mathbb{Z}_q^n$, $R_2 : \{0,1\}^* \to \mathbb{Z}_q$. Moreover, challenger C calls $AQRS.KeyExt$ to generate user's public key $L = \{p_1, p_2, \dots, p_l\}$ and secret key s, such that $\|s\| \le \vartheta\sqrt{m}$. ② C selects two matrices randomly $B \leftarrow \mathbb{Z}_q^{n\times m}$, $D \leftarrow \mathbb{Z}_q^{n\times m}$ then C sends (R_1, R_2, P_i, B, D) to the efficient attacker A.

(2) Query: The challenger C builds lists L_1, L_2, L_3, L_4 to store efficient attacker R_1 query, R_2 query, secret key s query, and signature query, respectively. Then, the efficient attacker A makes inquiries as following and C answers these inquiries. ① R_1 query: A chooses s_i from $\{s_1, s_2, \dots, s_l\}$, $i = 1, 2, \dots, l$ to send an inquiry. After that, C checks list L_1, and if A has asked for this information, s will return the same result to A. Otherwise, it returns L to A, and adds (P_i, s_i, L, T_i) to list L_1. ② R_2 query: A can enquire the message $\mu \in \{0,1\}^*$, $s = \{s_1, s_2, \dots, s_l\}$ and vectors $t_i \in D_\vartheta^{m+1}$. Then C checks the list L_2, and sets $\upsilon = c_1$, and then returns υ to A and puts (μ, R, T, υ) into list L_2, where $T = \{t_1, t_2, \dots, t_l\}$. It is worth mentioning that if A has asked for this information, C will return the same result to A as R_1 query. ③ Secret key query: First of all, A chooses the $s_i \in s$ to state secret key query. Then, C detects (P_i, s_i, L, T_i) in List L_1. Through $SamplePre$ algorithm, C computes the secret key s satisfying $P_i \cdot s = L \ mod \ q$, and sends s to efficient attacker A. Finally, A adds the two-tuples (s_i, s) in list L_3. ④ Signature query: To begin with, A selects the signer s_i, and asks C to compute a signature for message $\mu \in \{0,1\}^*$. After getting this signature query, C runs $SampleDom$ to randomly select vector $u \in \mathbb{Z}_q^{m+1}$, $t_i \in \mathbb{Z}_q^{m+1}$, $i = 1, 2, \dots, l$, such that $\|u\| \le \vartheta\sqrt{m+1}$ and $\|t_i\| \le \vartheta\sqrt{m+1}$. If u and t_i does not meet this condition, C will restart the process. Moreover, C calculates $R_1(s_i)$ as the public key of user s_i, named L. After that, C runs $SamplePre$ algorithm to get the secret key s satisfying $\|s\| \le \vartheta\sqrt{m}$, at the same time, C also calculates $R_2(D, s)$, named r_μ. Finally, C executes the $SigExt$ Algorithm and outputs the linkable ring signature $\vartheta_L(\mu) = (c_1, t_1, t_2 \cdots, t_l, R, P)$.

(3) Forgery: Firstly, A submits a message $\mu^* \in \{0,1\}^*$, the signature user identity is $s_i^* \in s^*$ and a forged ring signature $\vartheta_{L^*}(\mu) = (c_1^*, t_1^*, t_2^* \cdots, t_l^*, R, P)$ satisfying: ① The attacker A did not obtain the secret key of user s_i^*; ② The attacker A did not own the signature of (μ^*, L^*); ③ The public key of any users in ring L^* is given by the challenger C.

Analysis: Firstly, C queries the list L_2 of the efficient attacker A, if L_2 includes $(L^*, \mu^*, T^*, \upsilon^*)$, it will consider as a legitimate signature. Otherwise, C gives up this game. If $\vartheta_{L^*}(\mu^*)$ is a legitimate signature, we have:

$$\begin{aligned} &T_P^* t_k^* - [R_1(s_1^*)c_k^* + R_1(s_2^*)c_k^* + \cdots + R_1(s_l^*)c_k^*] \\ &= T_P^* t_k^* - [\sum_{i=1}^{l} R_1(s_i^*)] \cdot c_k^* = T_P^* t_k^* - T_P^* s^* c_k^* = T_P^* \cdot \mu^* \end{aligned} \tag{7}$$

$$\begin{aligned} &R_B^* t_k^* - [R_1(s_1^*)c_k^* + R_1(s_2^*)c_k^* + \cdots + R_1(s_l^*)c_k^*] \\ &= R_B^* t_k^* - [\sum_{i=1}^{l} R_1(s_i^*)] \cdot c_k^* = R_B^* t_k^* - R_B^* s^* c_k^* = R_B^* \cdot \mu^* \end{aligned} \tag{8}$$

Then, C obtains the secret key s^* of user. Let $t_i = t_i^*$, $i = 1, 2, \dots, k-1, k+1, \dots, l$ and computes $t_\pi = \mu + s_{2q,\pi} \cdot c_\pi \cdot (-1)^b$, so the signature $\vartheta_L(u) = (c_1, t_1, t_2, \dots, t_l, R, P)$ is also a legal signature. Thus we have:

$$T_P^* t_k - [R_1(s_1^*)c_k^* + R_1(s_2^*)c_k^* + \cdots + R_1(s_L^*)c_k^*] = T_P^* \cdot \mu^* \tag{9}$$

$$R_B^* t_k - [R_1(s_1^*)c_k^* + R_1(s_2^*)c_k^* + \cdots + R_1(s_L^*)c_k^*] = R_B^* \cdot \mu^* \tag{10}$$

From the above equations, we obtain: $T_P^* t_k - T_P^* t_k^* = 0 \mod q$ and $R_B^* t_k - R_B^* t_k^* = 0 \mod q$.

If $t_k - t_k^* \ne 0$, due to $\|t_k\| \le \vartheta\sqrt{m+1}$, $\|t_k^*\| \le \vartheta\sqrt{m+1}$, we have: $T_P^* t_k - T_P^* t_k^* = T_P^* \cdot \|t_k - t_k^*\| \le 2\vartheta^2(m+1)$.

We now conclude that $T_P^* t_k - T_P^* t_k^*$ is a solution to the SIS assumption, and if $t_k - t_k^* = 0$, C will give up the game.

Assuming that the probability is ε, which A can successfully forge a legitimate ring signature, and the probability of C successfully solving the SIS problem is ε^*. Thus, we have $\varepsilon^* = \varepsilon - \frac{1}{(2d)^l}$, equivalently, the challenger C can solve the SIS problem with probability $\varepsilon - \frac{1}{(2d)^l}$.

The unforgeability of the AQRS scheme dramatically confirms the authenticity and integrity of records of users' access to public places or contact with other users, preventing tampering or falsification by efficient attackers. Meanwhile, it also provides accuracy for contact tracing and status update, which prevents false reporting attacks for epidemic tracing. Furthermore, as shown in Fig. 1, we upload the records and signatures to the blockchain for storage. Due to the non-deletable and non-modifiable properties of blockchain data after uploading, the user's signature and its records are reassured to be unforgeable.

6.3. Unconditional anonymity

Theorem 5. *Our AQRS scheme is unconditionally anonymous for any efficient attacker A in polynomial time.*

Proof. It is completed through game between challenger C and efficient attacker A. C firstly inputs security parameter λ.

Case 1: (1) A inputs the message $\mu \in \{0,1\}^*$ which will be signed, the set of user identities $s = \{s_1, s_2, \dots, s_l\}$ and selects user s_1, s_2 for C. Then, C selects $b = 0$ and generates the secret key s. C supposes the actual signer $s_k = s_1$. (2) C processes $AQRS.SigExt$ algorithm and generates signature $\vartheta_L(\mu) = (c_1, t_1, t_2, \dots, t_l, R, P)$ and then sends it to A. After that, A will guess about b.

Case 2: (1) A inputs the message $\mu \in \{0,1\}^*$, the set of user identities $s = \{s_1, s_2, \dots, s_l\}$ and selects user s_1, s_2 for C. Then, C selects $b = 1$ and generates the secret key s. C supposes the actual signer $s_k = s_2$. (2) C executes the $AQRS.SigExt$ algorithm Sign, and generates signature $\vartheta_L^*(\mu) = (c_1^*, t_1^*, t_2^*, \dots, t_l^*, R, P)$ and sends it to A. After that, A will guess about b.

Analysis: For signature $\vartheta_L(\mu)$, we have $t_i \leftarrow D_\vartheta^{m+1}$, it can be seen from Lemma 3 that the signature $\vartheta_L(u) = (c_1, t_1, t_2, \dots, t_l, R, P)$ and $(D_\vartheta^{m+1})^{l+1}$ are indistinguishable statistically. The same can be obtained,

$\vartheta_L^*(\mu)$ and $(D_\vartheta^{m+1})^{l+1}$ are indistinguishable statistically. We obtain that $\vartheta_L(\mu)$ and $\vartheta_L^*(\mu)$ obey the same discrete Gaussian distribution [32], thus, $\vartheta_L(\mu)$ and $\vartheta_L^*(\mu)$ are indistinguishable statistically. A does not determine whether signature is generated by s_1 or s_2. Therefore, the advantage of efficient attacker A which can distinguish two signatures can be ignored.

In summary, our AQRS scheme satisfies the unconditional anonymity. It ensures the anonymity of health users, which maintains user privacy.

6.4. Linkability

Theorem 6. *Our AQRS scheme is linkable for any polynomial-time efficient attacker A.*

Proof. It is completed by one game between a challenger C and an efficient attacker A. We suppose that A can win the game with non-negligible advantage $Adv_A^{Linkability}$.

(1) C executes the $AQRS.Setup$ Algorithm to get public parameter (P, R) and sends it to A.

(2) A performs hash query, secret key query, and signature query to C by accessing oracles. Then, C returns result of every query to A.

① R_1 query: C returns L to A when A selects user $s_i \in s$ for inquiry. ② R_2 query : A selects the message $\mu \in \{0,1\}^*$, the ring $s = \{s_1, s_2, \ldots, s_l\}$ and vectors $t_i \in D_\vartheta^{m+1}$, $i = 1, 2, \ldots, l$ for inquiry. C sets c_1 and returns it to A. ③ Secret key query : First of all, A chooses the $s_i \in s$ to state secret key query. Through $SamplePre$ algorithm, C computes secret key s, and returns the secret key of user s_i to efficient attacker A. ④ Signature query: A selects signer $s_i \in s$, and also asks C to compute the signature of message μ. After getting this signature query, challenger C will execute $AQRS.SigExt$ algorithm by using the secret key s corresponding to s_i and also obtain signature $\vartheta_L(\mu)$, and finally return it to efficient attacker A.

(3) Attacker A has two valid signatures, named $\vartheta_{L_1}(\mu_1) = (c_1, t_1, t_2, \ldots, t_l, r_{\mu_1})$ and $\vartheta_{L_2}(\mu_2) = (c_1^*, t_1^*, t_2^*, \ldots, t_l^*, r_{\mu_2})$.

Analysis: Assuming that after A uses secret key, A will obtain two valid ring signatures $\vartheta_{L_1}(\mu_1)$ and $\vartheta_{L_2}(\mu_2)$ with a non-negligible probability ε. Since AQRS scheme is unforgeable and C inputs the same secret key $s = s'$, the efficient adversary A will always get the same output. Therefore, we get two tags $r_{\mu_1} = r_{\mu_2}$. This means that ring signatures $\vartheta_{L_1}(\mu_1)$ and $\vartheta_{L_2}(\mu_2)$ will return "Linked". It contradicts the assumption of Definition 8, so the advantage $Adv_A^{Linkability}$ of the efficient attacker A is negligible.

In a nutshell, our AQRS scheme satisfies the linkability under the Random Oracle Model. It contributes enormously to the epidemic infection control scheme, ensuring excellent traceability and efficiency in epidemiological investigation phase.

6.5. Non-slanderability

Theorem 7. *Our AQRS scheme satisfies the non-slanderability for all efficient PPT adversary A.*

Proof. Adversary A owns L_i, s_i, $i = 1, 2, \ldots, l$. First of all, A calculates a signature $\vartheta_{L_2}(\mu_2)$ with linkability label h_{μ_2}, which is linkable to the signature $\vartheta_{L_1}(\mu_1)$ generated by s_π. Thus, A gets the signature that is linkable to $\vartheta_{L_1}(\mu_1)$ without knowing the secret key s_π. Then, A also calculates a valid signature $\vartheta_{L_3}(\mu_3)$ with secret key s_i, $i = 1, 2, \ldots, l$, which is unlinkable to $\vartheta_{L_2}(\mu_2)$. Moreover, we send $\vartheta_{L_3}(\mu_3)$, $\vartheta_{L_2}(\mu_2)$ to the forger, and the forger will utilize them to get a solution of the SIS problem and then returns it to A. In particular, our AQRS scheme will be secure when the two valid and unlinkable signatures created by different users are utilized. As proved by Theorems 4 and 6, efficient attacker A will find a solution to the SIS problem with negligible probability. Therefore, the security analysis of unforgeability and linkability imply the non-slanderability of our scheme indirectly.

Table 2
Comparison of time costs.

Scheme	System key generation	User key generation
Our Scheme	$Time_{TG}$	$Time_{MUL} + Time_{SP}$
Baum et al. [37]	–	$Time_{MUL} + Time_{SD}$
Sun et al. [36]	–	$Time_{MUL} + Time_{SP}$
Jia et al. [38]	$Time_{TG}$	$Time_{MUL} + Time_{INV} + Time_{BD} + kTime_{SP}$

Scheme	Signature generation	Signature verification
Our Scheme	$(2l+1)Time_{MUL} + lTime_{SD}$	$2lTime_{MUL}$
Baum et al. [37]	$(3l+1)Time_{MUL} + lTime_{SD}$	$3lTime_{MUL}$
Sun et al. [36]	$(3l+2)Time_{MUL} + lTime_{SD}$	$(4l+1)Time_{MUL}$
Jia et al. [38]	$(l+1)Time_{MUL} + lTime_{SD}$	$3lTime_{MUL}$

Non-slanderability ensures the authenticity and correctness of two signature links, avoiding misreporting among close and sub-close contacts or social panic.

6.6. Anti quantum computing security

In our proposed secure epidemic control scheme, the lattice-based linkable ring signature primitive is utilized to perform the signatures on the related epidemic records. The lattice-based linkable ring signature in our scheme is can be reduced to the SIS hard problem, which in Definition 2. If that SIS hard problem is cracked, it means that our signature is no longer resistant to quantum attacks, but this is almost impossible until now. Therefore, our epidemic control scheme has the ability to resist quantum computing attacks.

7. Performance evaluation

In this paper, we introduce and propose a lattice-based linkable ring signature with link tags that is effective for epidemic contract tracing model.. In the existing studies, there is no privacy-preserving infection control scheme that can resist quantum attacks, hence we mainly evaluate the performance against three other lattice-based signature schemes [36–38] in terms of signatures performance. We conduct on Windows 10, AMD Ryzen 7 5800H with Radeon Graphics 3.20 GHz processor, 16.0 GB running in RAM, and our programming environment is Visual C++ 6.0. We set the parameters $n = 8$, $m = 640$, which is efficient and secure. Here, our security criteria is semantic security, i.e., any efficient PPT adversary cannot effectively distinguish the two different signatures.

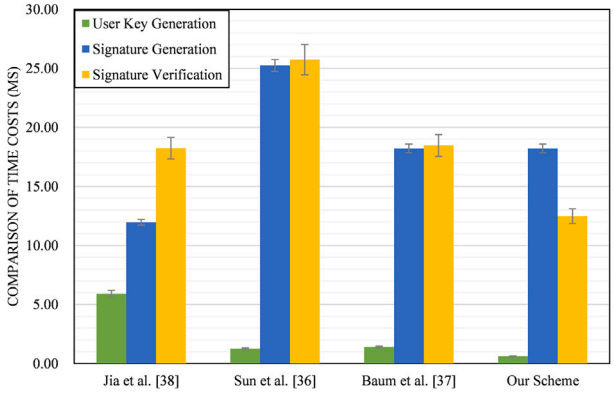


Fig. 6. Comparison of signature time costs.

7.1. Time consumption

Infection control requires a low time consumption to trace contacts of infected users rapidly. In this section, the time consumption of our scheme is evaluated against three other lattice-based signatures, as shown in Table 2. Besides, $Time_{TG}$, $Time_{SP}$, $Time_{SD}$, $Time_{BD}$,

$Time_{MUL}$, $Time_{INV}$ are represent the average single step time of the $TrapGen$, $SamplePre$, $SampleDom$, $BasisDel$ algorithm, scalar multiplication, and matrix inverse operation, respectively.

Both our scheme and scheme proposed by Jia et al. [38] use the $TrapGen$ algorithm $Time_{TG}$ for system key generation, while the schemes proposed by Sun et al. [36] and Baum et al. [37] consume almost zero in this part. Our scheme requires users to update their keys frequently. Therefore, in user key generation stage, we adopt hash function with short operation time to generate the user public key and call the original $SamplePre$ algorithm to generate the user secret key, so that the ring user key generation time is $Time_{SP}$. User public key in [38] is generated by the scalar multiplication and inverse operations of matrix, and the secret key is generated by invoking $BasisDel$ and $SamplePre$ algorithms. In contrast, the public key of [36] is generated from a randomly selected matrix and vector by the scalar multiplication operation, and the secret key is generated by Leftover Hash Lemma (LHL). The public key in the paper [37] is generated in approximately the same manner as in the paper [36], while the secret key is generated by $SampleDom$. Therefore, this leads to the calculation of the time overhead for the four schemes in Table 2.

In this paper, $2l$ scalar multiplications of matrices and vectors are required in the signature generation process, and $[l(m+1)]$-dimensional column vectors are randomly selected by calling $SampleDom$, with linkable tags I generated by calling a less time-consuming hash function. The generation time of linkable tags is negligible, hence our proposed AQRS scheme does not have any time overhead in the subsequent contact tracing process. The signature generation time overhead in [37] is similar to ours, while [36] has more $l+1$ matrix scalar multiplication operations than us, whereas our scheme has a slightly higher signature generation time overhead than that of [38]. In terms of signature verification, our scheme requires $2l$ scalar multiplications of matrices and vectors to be compared. The verification overhead of signature in our paper is also slightly lower than others.

Based on theoretical analysis, we evaluate the implementation of four lattice-based signature schemes, with assuming that ring members $l = 8$ and conducting experiments to compare three items of user key generation, signature generation and verification, respectively.. As shown in Fig. 6, Jia et al. [38] scheme has an overhead of only 11.96 (ms) for signature generation, but is too time-consuming for user key generation. In our privacy-preserving infection control scheme, users have to frequently update their keys, which will lead to excessive time overhead. Sun et al. [36] improved this problem, however, the time overhead of signature generation and verification is too onerous. Baum et al. [37] balances the above problems and will be more efficient and convenient when applied to infection control systems. For our scheme, it takes only 0.62 (ms) in signature generation, which is significantly lower than all lattice-based signature schemes. Our experimental results are basically consistent with the theoretical analysis, especially regarding the time overhead of key generation. In summary, our scheme has higher time efficiency in terms of user key generation, signature generation and verification.

7.2. Storage overhead

We compare and analyze the length of public key, secret key and signature with other schemes. In our scheme, the public key is an n-dimensional column vector generated by hashing the user's identity information.

The user public key of paper [38] composes of an $(n \times m)$-dimensional matrix generated by a scalar multiplication operation of two matrixes. The scheme of [36] consists of an $[n \times (m-1)]$-dimensional matrix with an n-dimensional column vector generated by a scalar multiplication operation with an $(m-1)$-dimensional column vector. The scheme in paper [37] user public key forms of an $(n \times m)$-dimensional matrix with an n-dimensional column vector generated by scalar multiplication operation with an m-dimensional column vector. Therefore, the length of the user public key of our scheme is almost equal to the papers [36,37], but significant diminish than the paper [38]. In terms of the length of the user secret key, user secret key in our scheme is an m-dimensional column vector, secret key in the scheme of [38] is an $(m \times k)$-dimensional matrix, secret key in the scheme of [36] is an $(m-1)$-dimensional column vector, and secret key in the scheme of [37] is an m-dimensional column vector, which shows similar performance of the four schemes as the user public key. In terms of signature length, the signature generated by our scheme is an $(m+1)$-dimensional column vector and the vector b is an n-dimensional column vector. As shown in Table 3, our scheme is approximately equal to the others in respect to the signature length.

Table 3
Comparison of storage overhead.

Scheme	User public key	User secret key	Signature
Our Scheme	$n\ log\ q$	$m\ log\ q$	$[(m+1)l+n]\ log\ q$
Baum et al. [37]	$n\ log\ q$	$m\ log\ q$	$(ml+n)\ \ log\ q$
Sun et al. [36]	$n\ log\ q$	$(m-1)\ log\ q$	$(ml+n)\ log\ q$
Jia et al. [38]	nm $log\ q$	$mk\ log\ q$	$(ml+k)\ log\ q$

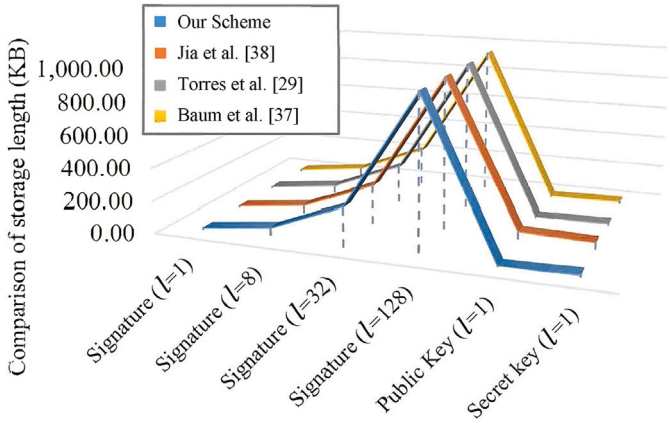


Fig. 7. Comparison of signature and public-secret key storage overhead with different number of ring members.

As shown in Fig. 7, we separately evaluated the signature length at $l = 1, l = 8, l = 32, l = 128$, respectively, public and secret key lengths at $l = 1$. With the increase of the number of ring members l, the growth of the signature lengths of the four schemes are roughly the same. However, the overheads of three schemes are basically comparable, except for the slightly higher scheme of Jia et al. [38] in terms of public and secret key length performance.

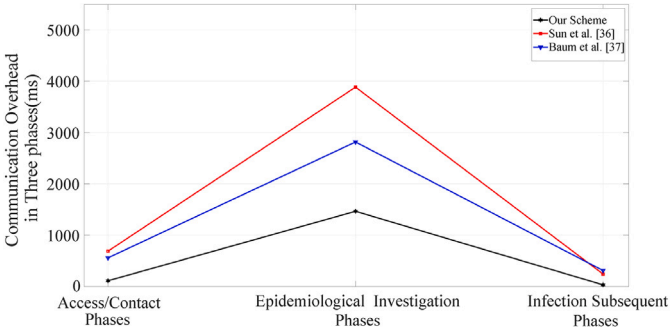


Fig. 8. Comparison of communication overhead.

7.3. Communication overhead

In privacy-preserving infection control systems, key generation, signature generation and signature verification are the main components of system communication overhead. Since [38] is lattice on identity-based ring signature has no linkable feature, we do not consider it as

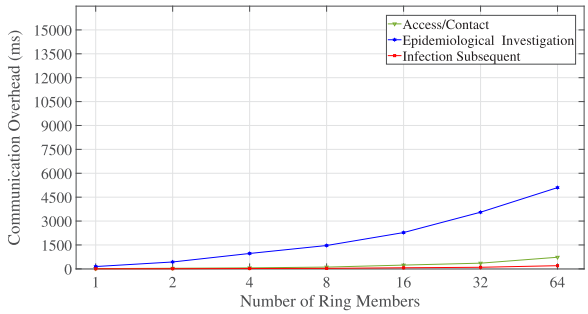


Fig. 9. Impact of number of ring members on system communication overhead.

a comparison. In this section, communication overhead will be evaluated and compared from three phases: User accessing public places or close contact with other users, Epidemiological investigation, Infection subsequent and timely updates.

In the experiments of time overhead, overhead of key generation, signature generation and verification of our scheme are obtained. We assume that the number of ring members $l = 8$ and each user is in close contact with 10 users in 14 days. This results in 10 close contacts of the infected patient and $10 \times 10 = 100$ sub-close contacts. Therefore, the MH requires a total of $10 + 100 = 110$ signatures to verify the linkable tags. In Accessing public places phase, users need to sign their access records, which is also required after verification of public place. Thus the communication overhead of this scheme in Accessing public places is $18.22 \times 2 + 12.48 \times 1 = 48.92$ (ms). Two close contact users in Contact phase need to sign and verify each other, taking a total of $18.22 \times 2 + 12.48 \times 2 = 61.40$ (ms). Thus, the total overhead of this phase is $48.92 + 61.40 = 110.32$ (ms). Epidemiological investigation phase is one of the most important and complex phases of infection control scheme. The infected user signs the result, hospital also requires confirmation by signature and MH has to verifies it. To ensure the safety of human being lives, IKG will stop providing services to infected persons after received and verified the signature from MH. The MH needs to track the close and sub-close contacts employing signature verification. Consequently, the communication overhead at this stage is $18.22 \times 3 + 12.48 \times 3 + 110 \times 12.48 = 1464.90$ (ms). In Infection subsequent and timely updates phase, system communication overhead is only $18.22 \times 1 + 12.48 \times 1 = 30.70$ (ms). According to same approach, the system communication overhead of applying the signature of the paper [36,37] can be derived. As shown in Fig. 8, our scheme has the lowest communication overhead in all three phases.

Meanwhile, we evaluated the communication overhead of each of the three phases with the number of ring members as a variable. As shown in Fig. 9, the communication overhead of the system grows as the number of ring members increases, especially in phase Epidemiological Investigation, the more frequently users contacts, the more difficult it is for the MH to conduct epidemiological investigations. In addition, we experimentally evaluated the effect of the number of users' close contacts on the communication overhead. As shown in Fig. 10, the overhead of the scheme increases as the number of close contacts of users increase, which is particularly evident in phase Epidemiological Investigation. In our scheme, the incremental overhead is manageable.

The scalability of our scheme is explained by combining Figs. 9 and 10. In general, scalability is the ability of a system to handle a growing workload, which in our paper to be considered as the load capacity of the scheme as the number of users increases in the epidemic control scenario. The communication overhead of our scheme is illustrated in Fig. 9 as the number of ring members growing. Since our scheme is distributed, in which each ring is computed in parallel, and since under normal circumstances an infected user is in close contact with several dozen users, the scalability of our scheme is optimized under such a conditional assumption. The trend of the scheme overhead with the increase of the number of close contacts of the infected users is shown in Fig. 10. As the number of users contacted by the infected users increases, the three indicators of scheme overhead rise slowly, not exponentially, and not even linearly. Hence, it concludes that our scheme has scalability without causing load problems.

8. Related work

The epidemic diseases have a wide-ranging impact in the world, with plenty scholars investigating the epidemic, especially how to control the spread of the epidemic in a timely manner. As shown in Table 4, we compare it with the existing COVID-19 control system [11, 19,39–42] and analyze their respective strengths and weaknesses.

Current researches have proposed several schemes such as [11] to track contacts for the purpose of controlling outbreaks. However, all these solutions suffer from a problem that they are based on centralized architectures, which is prone to the SPoF, DoS attacks and private data leakage. Meanwhile, some academics have proposed solutions that address the problems associated with the centralized architecture described above.

CAUDHT proposed by Samuel Brack [39] is a decentralized peer-to-peer system for contact tracking, which uses a Distributed Hash Table (DHT) to construct a distributed cryptographic messaging system for infected users and close contacts. However, their scheme does not take into account the protection against tracking attacks as well as the fact that the system suffers from a large storage overhead.

Paulo Valente Klaine [41] proposed a contact tracking framework by using blockchain, user privacy can be ensured while providing people with a full view of the infected individual. Nevertheless, the scheme does not contemplate efficient attackers tampering or forgery attacks and social panic.

BeepTrace [42] is a blockchain-enabled privacy-preserving contact tracking scheme proposed a tracking chain and a notification chain to effectively protect the privacy of all members, that mainly addresses the storage and throughput issues, yet the scheme completely fails to take into account the social panic attacks caused by record tampering forgery attacks.

The protocol proposed by Seham A. Alansari [19] was the best performing of the available studies, which differs from previous schemes by considering not only contact contacts but also public access and area recommendations, thus greatly improves infection control rates. Simultaneously, their system also considers other threats such as social graph leakage, stalking attacks and false reports. However, their proposed scheme does not cover the infected person treatment process and signatures are not linkable, which protects user privacy but does not perform optimally in terms of outbreak tracking.

Global quantum technologies evolve rapidly whereas none of the current privacy-preserving infection control schemes take into account the possibility of quantum information attacks. If quantum threats are not considered, this will be the maximum obstacle for future infection control and contact tracking systems. Collectively, our proposal outperforms existing systems, demonstrating impressive security, privacy and infection control.

9. Conclusion

In this paper, we propose a privacy-preserving epidemic infection control scheme by designing lattice-based linkable ring signature in blockchain. Our scheme is based on tracking close contacts and sub-close contacts as the primary method of epidemic infection control. Compared with current schemes, we record the time and locality of users accessing public places and coming into close contact with other users as well as taking into account the risks posed not only by close contacts but also by sub-close contacts. Moreover, we update and announce to the community about the trajectory of infected individuals and local risk levels promptly. Further, blockchain technology

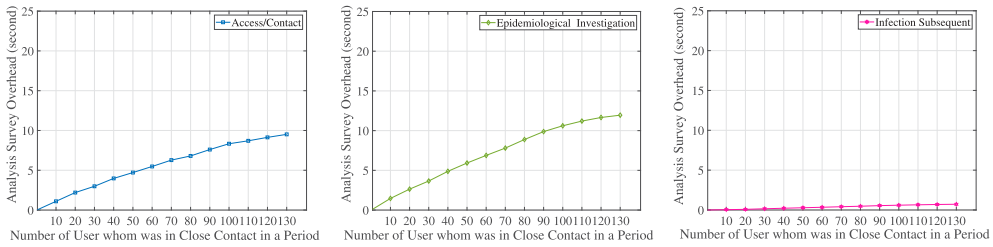


Fig. 10. Analyze the impact of the number of user contacts.

Table 4
Comparison between our scheme and other epidemic infection control schemes.

Comparison		T. Altuwaiyan et al. [11]	S. Brack et al. [39]	M. Torky et al. [40]	P. V. Klaine et al. [41]	H. Xu et al. [42]	S. A. Alansari et al. [19]	*Our Scheme*
Ordinary users	Anonymity	✓	✓	×	✓	✓	✓	✓
	Privacy protection for access or contact	∘	✓	×	✓	∘	✓	✓
	Prevent speculation on users' daily trajectories	✓	∘	×	✓	∘	✓	✓
Infected users	Disclosure the movements in 14 days	×	∘	×	×	×	×	✓
	Hospital quarantine	×	×	×	×	×	✓	✓
	Hospital treatment	×	×	×	×	✓	×	✓
Close contacts	Anonymity	×	✓	×	✓	∘	✓	✓
	Designated locality quarantine	×	×	×	×	×	∘	✓
Sub-close contacts	Anonymity	×	×	×	×	×	×	✓
	In-home quarantine	×	×	×	×	×	×	✓
Access in same time and locality with infected user	Anonymity	×	∘	×	✓	×	✓	✓
	Self-monitoring of health status	×	×	×	✓	×	∘	✓
Timely update of infection status and regional infection ranking		×	×	∘	✓	∘	✓	✓
Decentralized architecture		×	✓	✓	✓	✓	✓	✓
COVID-19 epidemic prevention and control transparency		∘	∘	∘	∘	∘	✓	✓
Contact tracing		✓	✓	✓	✓	✓	✓	✓
Prevention of false reporting by infected users		×	∘	✓	×	×	✓	✓
Factual authenticity of infection in infected users		×	×	×	×	×	∘	✓
Integrity of access and contact records		×	∘	×	∘	×	×	✓
Authenticity of access and contact records		×	∘	×	∘	×	×	✓
Effectiveness of infection control		∘	∘	∘	∘	∘	∘	✓
Preventing social panic attacks		×	∘	×	×	✓	✓	✓
Resistance to quantum computing attacks		×	×	×	×	×	×	✓
Signature to achieve linkability		×	×	×	×	×	×	✓
Signature to achieve unforgeability		×	×	×	×	×	∘	✓
Signature to achieve non-slanderability		×	×	×	×	×	×	✓

and lattice-based linkable ring signature enable our scheme to be extremely private, firmly semantic secure and outstanding traceability as well as resistant to quantum computing attacks. Security analysis and comprehensive performance evaluation demonstrate that our scheme fulfills the design goals with efficient time-consuming, storage consumption, and communication overhead. In a nutshell, our proposed scheme is practical and secure for epidemic and future pandemic privacy-preserving.

CRediT authorship contribution statement

Xue Chen: Conceptualization, Methodology, Validation, Investigation, Writing, Funding acquisition, Formal analysis, Review. **Shiyuan Xu:** Conceptualization, Methodology, Validation, Investigation, Writing, Funding acquisition, Formal analysis, Review. **Yibo Cao:** Methodology, Writing, Collected data, Data analysis, Review. **Yunhua He:** Funding acquisition, Visualization, Review, Editing, Supervision. **Ke Xiao:** Funding acquisition, Visualization, Review, Editing, Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgments

This work was supported in part by the R&D Program of Beijing Municipal Education Commission under Grant KM202010009010, in part by the National Natural Science Foundation of China under Grant 62272007, in part by the Beijing Municipal Natural Science Foundation under Grant M21029 and in part by the National Key Research and Development Program of China under Grant 2018YFB1800302.

References

[1] A.E. Gorbalenya, S.C. Baker, R.S. Baric, The species Severe acute respiratory syndrome-related coronavirus: classifying 2019-nCoV and naming it SARS-CoV-2, Nat. Microbiol. 5 (4) (2020) 536–544.

[2] World Health Organization, WHO coronavirus disease (COVID-19) dashboard, 2020, Available: https://covid19.who.int [Online].

[3] COVID-19 dashboard by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU), 2018, Available: https://coronavirus.jhu.edu/map.html [Online].

[4] Wuhan lockdown 'unprecedented', shows commitment to contain virus: WHO representative China, 2020, Available: https://www.reuters.com/article/us-china-healthwhoidUSKBN1ZM1G9 [Online].

[5] H. Tian, Y. Liu, Y. Li, C.-H. Wu, B. Chen, M.U. Kraemer, B. Li, J. Cai, B. Xu, Q. Yang, et al., An investigation of transmission control measures during the first 50 days of the COVID-19 epidemic in China, Science 368 (6491) (2020) 638–642.

[6] S. Chen, J. Yang, W. Yang, C. Wang, T. Bärnighausen, COVID-19 control in China during mass population movements at New Year, Lancet 395 (10226) (2020) 764–766.

[7] Wuhan municipal headquarters for the COVID-19 epidemic prevention and control, 2020, Available: http://www.xinhuanet.com/2020-01/21/c1125487978.htm [Online].

[8] G.F. Gensini, M.H. Yacoub, A.A. Conti, The concept of quarantine in history: from plague to SARS, J. Infect. 49 (4) (2004) 257–261.

[9] L. Ferretti, C. Wymant, M. Kendall, L. Zhao, A. Nurtay, L. Abeler-Dörner, M. Parker, D. Bonsall, C. Fraser, Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing, Science 368 (6491) (2020).

[10] Z. Wan, X. Liu, ContactChaser: A simple yet effective contact tracing scheme with strong privacy, IACR Cryptol. ePrint Arch. 2020 (2020) 630.

[11] T. Altuwaiyan, M. Hadian, X. Liang, EPIC: efficient privacy-preserving contact tracing for infection detection, in: 2018 IEEE International Conference on Communications, ICC, IEEE, 2018, pp. 1–6.

[12] L. Reichert, S. Brack, B. Scheuermann, Privacy-preserving contact tracing of COVID-19 patients, IACR Cryptol. ePrint Arch. 2020 (2020) 375.

[13] S. Xu, X. Chen, Y. He, Y. Cao, S. Gao, Vmt: secure vanets message transmission scheme with encryption and blockchain, in: Wireless Algorithms, Systems, and Applications: 17th International Conference, WASA 2022, Dalian, China, November 24–26, 2022, Proceedings, Part I, Springer, 2022, pp. 244–257.

[14] G. Xu, S. Xu, Y. Cao, F. Yun, Y. Cui, Y. Yu, K. Xiao, Ppseb: a postquantum public-key searchable encryption scheme on blockchain for e-healthcare scenarios, Secur. Commun. Netw. 2022 (2022).

[15] S. Nakamoto, A. Bitcoin, A peer-to-peer electronic cash system, Bitcoin 4 (2) (2008) URL: https://bitcoin.org/bitcoin.pdf.

[16] M. Castro, B. Liskov, Practical Byzantine fault tolerance and proactive recovery, ACM Trans. Comput. Syst. (TOCS) 20 (4) (2002) 398–461.

[17] S. Xu, X. Chen, Y. He, EVchain: An anonymous blockchain-based system for charging-connected electric vehicles, Tsinghua Sci. Technol. 26 (6) (2021) 845–856.

[18] C. Troncoso, M. Payer, J.-P. Hubaux, M. Salathé, J. Larus, E. Bugnion, W. Lueks, T. Stadler, A. Pyrgelis, D. Antonioli, et al., Decentralized privacy-preserving proximity tracing, IEEE Data Eng. Bull. 43 (2) (2020) 36–66.

[19] S.A. Alansar, M.M. Badr, M. Mahmoud, W. Alasmary, Efficient and privacy-preserving infection control system for Covid-19-like pandemics using blockchain, IEEE Internet Things J. (2021).

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

[21] D. Chaum, E. Van Heyst, Group signatures, in: Workshop on the Theory and Application of of Cryptographic Techniques, Springer, 1991, pp. 257–265.

[22] J.K. Liu, V.K. Wei, D.S. Wong, Linkable spontaneous anonymous group signature for ad hoc groups, in: Australasian Conference on Information Security and Privacy, Springer, 2004, pp. 325–335.

[23] N. Alkeilani Alkadri, P. Das, A. Erwig, S. Faust, J. Krämer, S. Riahi, P. Struck, Deterministic wallets in a quantum world, in: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, 2020, pp. 1017–1031.

[24] Y. Cao, S. Xu, X. Chen, Y. He, S. Jiang, A forward-secure and efficient authentication protocol through lattice-based group signature in vanets scenarios, Comput. Netw. 214 (2022) 109–149.

[25] S. Xu, X. Chen, C. Wang, Y. He, K. Xiao, Y. Cao, A lattice-based ring signature scheme to secure automated valet parking, in: Wireless Algorithms, Systems, and Applications: 16th International Conference, WASA 2021, Nanjing, China, June 25–27, 2021, Proceedings, Part II, Springer, 2021, pp. 70–83.

[26] S.A. Vanstone, R.J. Zuccherato, Elliptic curve cryptosystems using curves of smooth order over the ring Z/sub n, IEEE Trans. Inform. Theory 43 (4) (1997) 1231–1237.

[27] P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Rev. 41 (2) (1999) 303–332.

[28] T.D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, J.L. O'Brien, Quantum computers, Nature 464 (7285) (2010) 45–53.

[29] W.A.A. Torres, R. Steinfeld, A. Sakzad, J.K. Liu, V. Kuchta, N. Bhattacharjee, M.H. Au, J. Cheng, Post-quantum one-time linkable ring signature and application to ring confidential transactions in blockchain (lattice RingCT v1. 0), in: Australasian Conference on Information Security and Privacy, 2018, pp. 558–576.

[30] J. Howe, A. Khalid, C. Rafferty, F. Regazzoni, M. ONeill, On practical discrete Gaussian samplers for lattice-based cryptography, IEEE Trans. Comput. 67 (3) (2016) 322–334.

[31] J. Hoffstein, J. Pipher, J.H. Silverman, NSS: An NTRU lattice-based signature scheme, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2001, pp. 211–228.

[32] C. Gentry, C. Peikert, V. Vaikuntanathan, Trapdoors for hard lattices and new cryptographic constructions, in: Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing, 2008, pp. 197–206.

[33] V. Lyubashevsky, Lattice signatures without trapdoors, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2012, pp. 738–755.

[34] S. Agrawal, D. Boneh, X. Boyen, Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE, in: Annual Cryptology Conference, 2010, pp. 98–115.

[35] X. Chen, S. Xu, T. Qin, Y. Cui, S. Gao, W. Kong, AQ–ABS: Anti-quantum attribute-based signature for EMRs sharing with blockchain, in: 2022 IEEE Wireless Communications and Networking Conference, WCNC, IEEE, 2022, pp. 1176–1181.

[36] S.-F. Sun, M.H. Au, J.K. Liu, T.H. Yuen, Ringct 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero, in: European Symposium on Research in Computer Security, Vol. 10493, Springer, 2017, pp. 456–474.

[37] C. Baum, H. Lin, S. Oechsner, Towards practical lattice-based one-time linkable ring signatures, in: International Conference on Information and Communications Security, Springer, 2018, pp. 303–322.

[38] X. Jia, D. He, Z. Xu, et al., An efficient identity-based ring signature scheme over a lattice, J. Cryptol. Res. 4 (04) (2017) 392–404.

[39] S. Brack, L. Reichert, B. Scheuermann, Caudht: decentralized contact tracing using a DHT and blind signatures, in: 2020 IEEE 45th Conference on Local Computer Networks, LCN, IEEE, 2020, pp. 337–340.

[40] M. Torky, A.E. Hassanien, COVID-19 blockchain framework: innovative approach, 2020, arXiv preprint arXiv:2004.06081.

[41] P.V. Klaine, L. Zhang, B. Zhou, Y. Sun, H. Xu, M. Imran, Privacy-preserving contact tracing and public risk assessment using blockchain for COVID-19 pandemic, IEEE Internet Things Mag. 3 (3) (2020) 58–63.

[42] H. Xu, L. Zhang, O. Onireti, Y. Fang, W.J. Buchanan, M.A. Imran, Beeptrace: Blockchain-enabled privacy-preserving contact tracing for covid-19 pandemic and beyond, IEEE Internet Things J. 8 (5) (2020) 3915–3929.

Xue Chen is currently pursuing her M.Phil. degree at Department of Computing, The Hong Kong Polytechnic University, Hong Kong. Before she came to Hong Kong, she received the B.Eng. in Information Security at North China University of Technology, Beijing, China. Her research interests include applied cryptography, lattice, blockchain and information security. She has published several academic papers in refereed international conferences and premier journals include COMPUTER NETWORKS, WASA, IEEE WCNC, IEEE ICC and TSINGHUA SCIENCE AND TECHNOLOGY, etc. She won the Excellent Paper Award of TSINGHUA Science and Technology in 2022.

Shiyuan Xu is currently pursuing the Ph.D. degree at Department of Computer Science, The University of Hong Kong, Hong Kong. Before he came to Hong Kong, he received the B.Eng. in Information Security at North China University of Technology, Beijing, China. He was a summer research student at The University of Hong Kong in 2021. His research interests include post-quantum cryptography, blockchain and information security. He has published several academic articles in refereed international conferences and journals, such as COMPUTER NETWORKS, WASA, IEEE WCNC, IEEE ICC, Security and Communication Networks, and Peer-to-Peer Networking and Applications. He has served as a reviewer for many journals, including IEEE Transactions on Intelligent Transportation Systems, IEEE Access, Peer-to-Peer Networking and Applications, IEEE System Journal, etc. He won the Excellent Paper Award of TSINGHUA Science and Technology in 2022.

Yibo Cao is currently pursuing the M.Sc. degree at School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing, China. Before that, he received the B.Eng. in Information Security at North China University of Technology, Beijing, China. His research interests include blockchain, post-quantum cryptography and information security. He has published several academic papers in refereed international conferences and journals include COMPUTER NETWORKS, Security and Communication Networks, WASA 2021.

Yunhua He received the Ph.D. degree in computer science from Xidian University, Xi'an, China, in 2016. He has been an Associate Professor with the North China University of Technology, China. His research interests include security and privacy in cyber–physical systems, Bitcoin-based incentive mechanism, security and privacy in vehicle ad hoc networks. He has published 50 research articles in refereed international conferences and premier journals. He received the Best Paper Award from the conference WASA 2017. He won the Excellent Paper Award of TSINGHUA Science and Technology in 2022.

Ke Xiao received the Ph.D. degree from Beijing University of Posts and Telecommunications in 2008. He is currently a professor with the North China University of Technology. His research interests include blockchain and information security.