

Efficient privacy-preserving personal health record sharing framework based on decentralized lattice-based encryption

Chuai Yi¹ (✉), Zhang Leyou¹, Li Quanjiang²

1. School of Mathematics and Statistics, Xidian University, Xi'an 710126, China

2. School of Automation, Xi'an University of Posts and Telecommunications, Xi'an 710121, China

Abstract

To ensure the confidentiality of Internet of things (IoT) cloud data while enabling fine-grained access control, attribute-based encryption (ABE) schemes have been widely adopted. Despite their advantages, existing approaches suffer from three critical shortcomings: reliance on a central authority (CA) for key distribution which may lead to a single point of failure, dependence on mathematical hard problems like discrete logarithms and bilinear pairings which leaves most of them vulnerable to quantum attacks, and insufficient attention to user privacy protection mechanisms in current lattice-based ABE designs. To address these limitations, this article proposes a privacy-preserving personal health record (PHR) sharing framework based on lattice-based multi-authority attribute-based encryption (MA-ABE). The framework enhances user privacy through an anonymous commitment protocol that conceals identities and a key generation algorithm that allows decentralized authorities to issue private keys without exposing user information. Furthermore, the design extends beyond conventional single-attribute-per-authority models, enabling each authority to manage multiple attributes. Moreover, two-way anonymity for both provers and verifiers is achieved through these user privacy protection mechanisms. The proposed scheme achieves indistinguishability under selective-attribute chosen plaintext attack (IND-sAtt-CPA) security, while maintaining acceptable computational efficiency.

Keywords multi-authority(MA), smart health, lattice-based encryption, privacy-preserving

1 Introduction

IoT devices enable smart healthcare through remote monitoring and PHR collection. Data generated by wearable devices and hospital visits are stored on cloud servers, as shown in Fig. 1. A report stated that

approximately 902 million healthcare records were exposed in China in 2023, including identities, phone numbers, addresses, and confidential business data (<https://www.ciiabd.org.cn/articles/6g0X6g.html>). ABE^[1], including key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE)^[2], provides data confidentiality and fine-grained access control. In KP-ABE, access policies are embedded in secret keys, while ciphertexts are associated with attributes; decryption succeeds only when the attributes satisfy the policy.

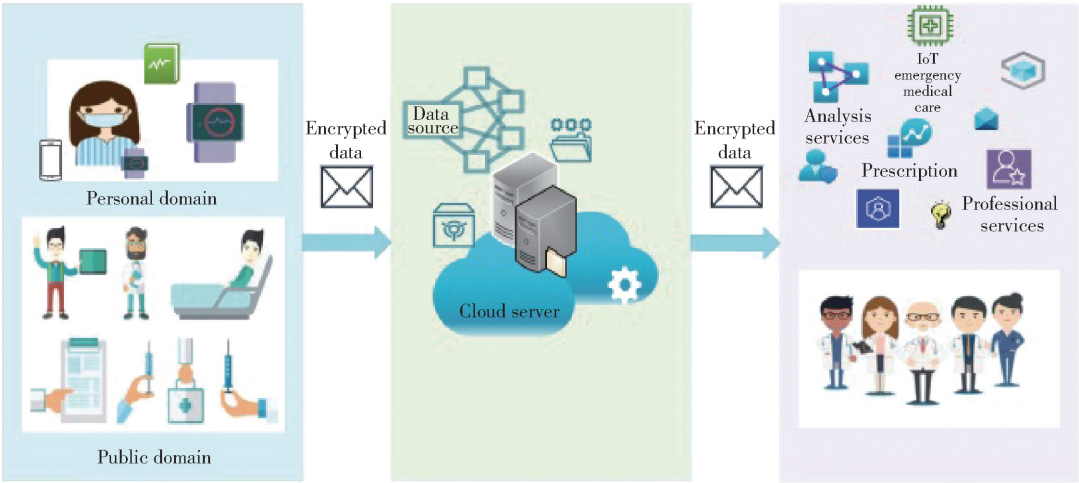


Fig. 1 PHR system

Most healthcare ABE schemes rely on bilinear pairings^[3-6], which are threatened by the quantum algorithms of Shor^[7] and Grover^[8]. Post-quantum cryptography (PQC)^[9] includes code-based, Hash-based, and lattice-based primitives^[10]. Among them, lattice-based cryptography offers efficient encryption, compact keys, and relatively simple implementation.

Existing lattice-based ABE schemes commonly depend on a central authority (CA)^[11-18]. Schemes^[11-13] use a fully trusted CA, whereas schemes^[14-18] adopt CA-assisted multi-authority architectures. Such centralization is unsuitable for cross-hospital policies managed by independent departments. Moreover, authorities receiving users' global identities (GIDs) during key issuance may track or impersonate users. Existing lattice-based anonymity mechanisms mainly employ group or blind signatures^[19-22], which generally provide only one-sided anonymity.

Therefore, a privacy-preserving MA-KP-ABE framework for PHR sharing is proposed. Its main contributions are as follows.

1) Practical construction. Most existing lattice-based schemes adopt either a single CA or CA + MA architecture. Our scheme employs a decentralized multi-authority construct, which mitigates single points of failure and key delegation issues caused by reliance on CAs. To improve efficiency, we extend the existing decentralized design^[23] from one-authority-to-per-attribute management to one-authority-managing-multi-

attribute management. In the multi-attribute setting, the key generation time is reduced.

2) Privacy protection. Our scheme ensures user anonymity when accessing the PHR-sharing platform. Users interact with the authorities to generate secret keys via an anonymous key generation algorithm. This algorithm ensures that the user's GID remains hidden, preventing a compromised authority from inferring attribute information by tracking GIDs.

3) Good trade-off between security and efficiency. Theoretical analysis demonstrates that our scheme achieves reasonable computational and storage overheads. Simulation results show that the performance of our scheme is acceptable. Moreover, the security proof shows that the proposed scheme is IND-sAtt-CPA secure under the evasive learning with errors (e-LWE) assumption.

2 Related work

2.1 MA-ABE

The first MA-ABE scheme^[24] distributed attributes among multiple authorities but retained a CA, whereas Ref. [25] achieved full decentralization. The first lattice-based MA-ABE scheme^[14] also relied on a CA. Ref. [26] introduced monotone access trees through Shamir secret sharing, while Ref. [27] supported linear secret-sharing scheme (LSSS) but fixed the authorities after system setup.

Ref. [28] proposed a decentralized LWE-based MA-ABE scheme supporting disjunctive normal form (DNF) policies in the random-oracle model. Ref. [23] strengthened its security and introduced more flexible subset policies, but restricted each authority to one attribute. Ref. [29] reduced public- and private-key sizes through two-step sampling. Refs. [17–18] respectively introduced revocation and LSSS-based access policies, but both still require a CA.

2.2 MA-ABE with privacy-preserving

The original MA-ABE scheme^[24] provides no user-privacy protection. Ref. [30] introduced anonymous key issuance using two-party computation and proof of knowledge, but requires authority cooperation and pairwise shared secrets. Ref. [31] removed the CA and enabled authorities to issue keys without learning users' GIDs. Ref. [32] concealed both GIDs and access policies, although its AND/OR access structure is limited.

Ref. [33] further protected both GIDs and attributes through two-party computation and zero-knowledge proofs; however, Ref. [34] showed that its basic model is vulnerable to collusion. Ref. [35] proposed an unpaired certificate-less signcryption scheme with enhanced privacy for vehicular networks.

Post-quantum anonymous schemes still face interaction, unlinkability, or bilateral-privacy limitations. Ref. [36] requires multiple verification rounds, whereas Ref. [37] provides non-interactive anonymity in the random-oracle model but does not support pseudonym-based bilateral privacy. Ref. [38] introduced commit-transferable signatures (CTS), combining commitments, signatures, and non-interactive zero-knowledge (NIZK) proofs to protect GIDs and, through encoding, user attributes.

In summary, existing schemes often rely on bilinear pairings, retain centralized key distribution, or provide insufficient user privacy.

3 Preliminaries

3.1 Notations

Let $\mathbb{Z}$ and $\mathbb{Z}_q$ denote the integers and integers mod q

respectively, and let $[N] = \{1, 2, \dots, N\}$. The security parameter is denoted by λ , and $g_{\text{negligible}}(\lambda)$ denotes a negligible function. Uppercase and lowercase bold letters denote matrices and vectors, respectively. For a matrix $\mathbf{K} = [\mathbf{k}_1, \dots, \mathbf{k}_m]$, let $\|\mathbf{K}\| = \max_i \|\mathbf{k}_i\|$, and for a vector $\mathbf{v}$, let $\|\mathbf{v}\|_\infty = \max_i |v_i|$. $D_{\mathbb{Z}, \chi}$ denotes the discrete Gaussian distribution over $\mathbb{Z}$ with parameter χ . $x \leftarrow_R \chi$ denotes random sampling from χ , and $\chi \approx_s \gamma$ indicates that two distributions are statistically close. Moreover, $x \leftarrow A_\chi^{-1}(\gamma)$ denotes sampling a short preimage satisfying $\mathbf{A}x = \gamma \bmod q$.

3.2 Lemmas and facts

Assumption 1 Decisional LWE^[39]: under appropriate lattice parameters, the distribution $(\mathbf{A}, \mathbf{A}s + e)$ is computationally indistinguishable from the uniform distribution over the corresponding domain.

Assumption 2 Evasive LWE^[23]: under the specified lattice parameters, no probabilistic polynomial-time adversary can distinguish the pre-challenge and post-challenge experiments with more than negligible advantage.

Theorem 3 Trapdoor generation^[40]: the algorithm $T_{\text{TrapGen}}(1^n, q, m)$ outputs a matrix $\mathbf{A}$ statistically close to uniform and a corresponding trapdoor t_{id_A} which supports efficient short-preimage sampling.

Fact 4 Gaussian norm bound^[23]: for a vector sampled from the specified discrete Gaussian distribution, its norm is bounded by $\sqrt{m}\omega$ except with negligible probability.

Lemma 5 Statistical closeness^[41]: under the specified lattice and Gaussian parameters, the distributions ψ_1 and ψ_2 defined above are statistically close, i. e., $\psi_1 \approx_s \psi_2$.

Definition 6 Hiding property^[42]: a commitment scheme is computationally hiding if no probabilistic polynomial-time adversary can distinguish commitments to any two equal-length messages with more than negligible advantage.

Definition 7 NIZK proof system (<https://www3.cs.stonybrook.edu/~omkant/L20-short.pdf>): an

NIZK system enables a prover to prove that a statement belongs to a language without revealing its witness. It satisfies completeness, soundness, and zero knowledge.

4 System overview

4.1 System model

As shown in Fig. 2, the scheme involves five entities: data owners, data users (typically doctors or researchers), the PHR-sharing platform, organization O , and hospitals.

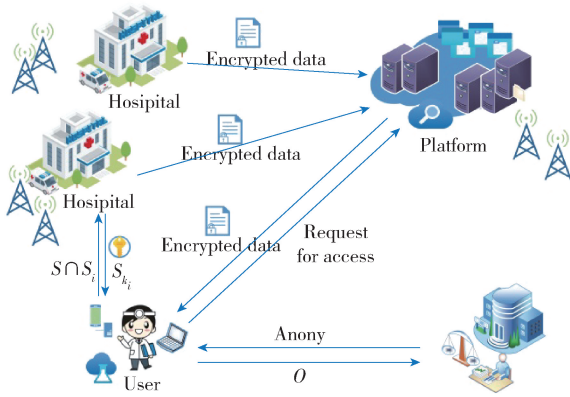


Fig. 2 System model

Their roles are as follows:

- 1) Data owners: patients whose hospital visits generate personal health records (PHRs).
- 2) Data users: doctors or researchers who request PHRs from the sharing platform or hospitals. The requested data are returned in encrypted form and can be decrypted only by users satisfying the access policy. Data users may also obtain anonymous credentials from organization O to prove their legitimacy without revealing their GIDs.
- 3) Authorities: authorities are corresponding departments across hospitals, such as neurosurgery. They record diagnosis and treatment data as PHRs, anonymize patients' identities and sensitive information for research use, encrypt the anonymized PHRs, and upload them to the platform. They also define access policies, issue decryption keys to eligible users, and verify anonymous users' legitimacy. Fig. 3 shows an

example access structure.

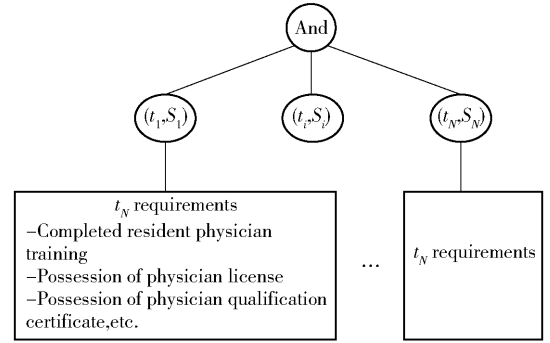


Fig. 3 Access policy

4) PHR-sharing platform: an honest-but-curious cloud server that stores encrypted PHRs and provides them to authorized users.

5) Organization O : a fully trusted entity that issues anonymous credentials to doctors or researchers, enabling them to prove their legitimacy to checkers.

4.2 Algorithms definition

- 1) $G_{\text{GlobalSetup}}(1^\lambda) \rightarrow g_{\text{gp}}$. Input the security parameter λ , and this algorithm generates the global parameter g_{gp} .
- 2) $A_{\text{AuthoritySetup}}(g_{\text{gp}}, \theta) \rightarrow (p_{k_\theta}, m_{sk_\theta}, A_\theta)$. Provide the global parameter g_{gp} and the authority identifier θ as input, each authority generates its public key p_{k_θ} and its secret key m_{sk_θ} . A_θ is an access structure define by authority θ .
- 3) $K_{\text{KeyGen}}(g_{\text{gp}}, \text{GID}, S, p_{k_\theta}, m_{sk_\theta}, A_\theta) \rightarrow s_{k_{\text{GID}, \theta}}$. This algorithm takes global parameter g_{gp} , user identifier GID, user attribute set S , authority public key p_{k_θ} , and master key m_{sk_θ} as input. This algorithm outputs secret key $s_{k_{\text{GID}, \theta}}$ for S depends on A_θ .
- 4) $E_{\text{Encrypt}}(g_{\text{gp}}, p_{k_\theta}, \mu, S \cap S_\theta) \rightarrow c_{t_\theta}$. This algorithm takes global parameter g_{gp} , authority public key p_{k_θ} , intersection of user attribute set S authority attribute set S_θ , a message $\mu \in \{0, 1\}$ as input. It outputs the ciphertext c_{t_θ} .
- 5) $D_{\text{Decrypt}}(g_{\text{gp}}, s_{k_{\text{GID}, \theta}}, c_{t_\theta}) \rightarrow m_\theta$. If the user attribute S satisfies the A_θ specified by authority θ , then the private key $s_{k_{\text{GID}, \theta}}$ obtained from authority θ is well-formed. The algorithm can successfully output the plaintext m_θ .

Correctness

The proposed MA-ABE scheme is correct if for an arbitrary message $\mu \in \{0, 1\}$, any access policy A_θ , when S satisfies A_θ , the following equation holds:

$$\Pr[D_{\text{Decrypt}}(E_{\text{Encrypt}}(g_{\text{gp}}, p_{k_\theta}, \mu, S \cap S_\theta), p_p, s_{k_{\text{CID}, \theta}})] = 1 - g_{\text{negligible}}(\lambda) \quad (1)$$

4.3 Security model

The IND-sAtt-CPA security is illustrated by the game between the challenger $\mathcal{C}$ and the adversary $\mathcal{A}$. Before the system set up, the challenge attribute set $\mathcal{G}^*$ and the corrupt authorities set Cor need to be supplied by the adversary $\mathcal{A}$. It is required that the authorities in Cor can not manage the attribute set $\mathcal{G}^*$.

1) Initialization. The adversary $\mathcal{A}$ declares the challenge attribute set $\mathcal{G}^*$. The challenger $\mathcal{C}$ invokes $G_{\text{GlobalSetup}}(1^\lambda)$ to obtain public parameters g_{gp} . He then sends g_{gp} to the adversary $\mathcal{A}$.

2) Set up. The challenger $\mathcal{C}$ invokes $A_{\text{AuthoritySetup}}(1^\lambda)$ to obtain authorities' public parameters p_k and master key s_k . $\mathcal{C}$ sends p_k and $\{s_{k_\theta}\}_{\theta \in \text{Cor}}$ to $\mathcal{A}$.

3) Phase-1. The adversary $\mathcal{A}$ arbitrarily chooses the access structure $\mathbb{W}$ for querying private keys. It is required that $\mathcal{G}^*$ cannot satisfy $\mathbb{W}$. The challenger $\mathcal{C}$ invokes K_{KeyGen} and sends the sampling result $s_{k_{\text{CID}, \theta}}$ to $\mathcal{A}$.

4) Challenge. $\mathcal{A}$ outputs the challenge messages μ_0 and μ_1 with the same length. The challenger $\mathcal{C}$ selects $b \in \{0, 1\}$ and generates c_t under $E_{\text{Encrypt}}(g_{\text{gp}}, \mathcal{G}^*, \mu_b, p_k)$. Then the challenger sends c_t to $\mathcal{A}$.

5) Phase-2. Similar as Phase-1. It is required that $\mathcal{G}^*$ can not satisfy the challenge access structure $\mathbb{W}$.

6) Guess. $\mathcal{A}$ outputs $b' \in \{0, 1\}$. $\mathcal{A}$ wins the game if and only if $b' = b$.

4.4 Anonymous credential system

The anonymous credential system combines a commit-transferable signature (CTS) scheme with a NIZK proof system and follows the constructions in Refs. [38–39]. Its main procedures are summarized as follows.

1) ACS. setup. The organization O generates the public parameters for the CTS and NIZK systems and runs the CTS key-generation algorithm to obtain the key pair (p_{k_0}, s_{k_0}) .

2) ACS. register. The user U commits to its secret input usk to obtain c_{comm} and generates an NIZK proof π of the commitment's well-formedness. U sends the pseudonym $\text{anony} = (c_{\text{comm}}, \pi)$ to O , which accepts the registration if the NIZK verification succeeds.

3) ACS. issue. After successful registration, O signs c_{comm} using the CTS signing algorithm and returns the resulting signature σ as the credential Cred . The user's secret input is not disclosed.

4) ACS. prove. To prove credential ownership under a fresh pseudonym, U transforms σ into σ' . randomizes c_{comm} into $c_{\text{comm}'}$, and generates an NIZK proof π' for $c_{\text{comm}'}$. U then sends $\text{anony}' = (c_{\text{comm}'}, \sigma')$ and π' to the verifier.

5) ACS. verify. The verifier accepts the credential if both the CTS verification of σ' and the NIZK verification of π' succeed; otherwise, it rejects.

5 Construction of PHR sharing system

5.1 Description of the notations

Table 1 gives a list of notations in our construction.

Table 1 Description of notations

Notation	Description
n, m, q, χ	lattice parameters that are related to λ
χ_{PRF}	Gaussian width parameter
$\mathbf{K}_0, \mathbf{K}_1$	Two matrices sampled from $D_{Z, \chi_{\text{PRF}}}^{m \times m}$
$I = I(\lambda)$	The bit string length of the identity
$L = L(\lambda)$	A count of the number of attributes in a ciphertext
GID	The identifier of the user
A_{A_θ}	The identifier of the authority θ
S_θ	The attribute set managed by A_{A_θ}
H	A Hash function
j_θ	The attribute managed by A_{A_θ}
g_{j_θ}	The random number associated with j_θ
$s_{\text{sk}_{\text{anony}', \theta}}$	Partial secret key issued by A_{A_θ} for pseudonym anony'
$p_{k_\theta}, m_{sk_\theta}$	The public key and secret key of A_{A_θ}

5.2 Construction

Phase 1 Global setup

This algorithm takes the system security parameter λ as input, selects lattice parameters n, m, q, χ , a Gaussian width parameter χ_{PRF} , an identity string bit-length function $I = I(\lambda)$, and two matrices $\mathbf{K}_0, \mathbf{K}_1$ sampled from $D_{Z, \chi_{\text{PRF}}}^{m \times m}$. Let H be a Hash function that maps user identity GID to elements in Z_q^m , i. e. $H: \{0, 1\}^I \rightarrow Z_q^m$. The function H is instantiated by

$$H(x) = \left(\prod_{i \in [I]} \mathbf{K}_{x_i} \right) \mathcal{E} \quad (2)$$

where $\mathcal{E} = (1, 0, \dots, 0)^T \in Z_q^m$. Finally, the system outputs the public parameters $g_{\text{gp}} = (H, \mathbf{K}_0, \mathbf{K}_1, I, \lambda, n, m, q, \chi, \chi_{\text{PRF}})$.

Phase 2 Authority setup

1) Initial setting of authorities

The proposed construction supports multiple attribute authorities. There are N authorities in this system, denoted as $A_{A_1}, A_{A_2}, \dots, A_{A_N}$. The attribute sets managed by them are denoted as $S_1, S_2, \dots, S_N$ respectively. Each authority sets its threshold, denoted as $t_1, t_2, \dots, t_N$ separately. Each authority selects one random number associated with one attribute managed. g_{j_θ} is the random number corresponding to attribute j_θ , and this number can be disclosed.

2) Public-private key generation for authorities

The authority A_{A_θ} invokes the trapdoor generation algorithm to generate a matrix $\mathbf{A}_\theta^M$ and its corresponding trapdoor t_{d_θ} . $T_{\text{TrapGen}}(1^n, q, m) \rightarrow (\mathbf{A}_\theta^M, t_{d_\theta})$. Subsequently, the authority randomly selects a vector $\mathbf{p}_\theta \leftarrow_R Z_q^n$, $\mathbf{B}_\theta \leftarrow_R Z_q^{n \times m}$. The authority then outputs the public key $p_{k_\theta} = (\mathbf{A}_\theta^M, \mathbf{B}_\theta, \mathbf{p}_\theta)$ and master private key $m_{sk_\theta} = t_{d_\theta}$, which is securely stored by the authority.

Phase 3 Anonymous registration of users

The anonymous user registration phase is shown in Algorithm 1.

Algorithm 1 User registration

Input: the user's identifier GID , public parameters g_{gp} , the public key p_{k_O} and master key s_{k_O} of organization O .

Ensure: the user's anonymous credential σ' .

1: **User U do:**

2: Calculate the commitment: $\text{Commit}(\text{GID}, p_{\text{params}}, \text{Rand}) \rightarrow$

$c_{\text{comm}}.$

3: Generate zero-knowledge proofs; NIZK. $\text{Prove}(p_{\text{params}}, c_{\text{comm}}, \text{GID}, r_{\text{Rand}}) \rightarrow \pi.$

4: Send $\text{anony} = (c_{\text{comm}}, \pi)$ to O .

5: **Organization O do:**

6: Verify the zero-knowledge proof NIZK. $\text{Verify}(c_{\text{comm}}, \pi)$

7: **If** the verification passes, **then**

8: Generate the signature CTS. $\text{Sign}(p_{\text{params}}, s_{k_O}, c_{\text{comm}}) \rightarrow \sigma.$

9: Send σ to U .

10: **End if.**

11: **User U do:**

12: **Randomize the commitment:** CTS. $\text{Randomize}(c_{\text{comm}}, r_{\text{Rand}}, r_{\text{Rand}}') \rightarrow c_{\text{comm}}'.$

13: **Convert the signature:** Transfer $(p_{\text{params}}, p_{k_O}, G_{\text{GID}}, \sigma, r_{\text{Rand}}, r_{\text{Rand}}') \rightarrow \sigma'.$

14: Generate new proofs; NIZK. $\text{Prove}(c_{\text{comm}}') \rightarrow \pi'.$

15: Send $\text{anony}' = (c_{\text{comm}}', \pi')$ to A_θ .

16: A_θ do:

17: Verify the signature CTS. $\text{Verify}(p_{\text{params}}, p_{k_O}, c_{\text{comm}}', \sigma')$

18: Check the proof π .

19: **If** the verification passes, **then**

20: accept the anonymous credential $\sigma'.$

21: **End if.**

22: Return $\sigma'.$

1) User commitment. A user U with identity GID inputs the public parameters of the commitment algorithm Commit , selects a random number r_{Rand} , executes the commitment algorithm in Algorithm 1 to generate a commitment value comm , and uses the NIZK. Prove algorithm to generate a zero-knowledge proof π for c_{comm} . The user U constructs the pseudonym $\text{anony} = (c_{\text{comm}}, \pi)$ and sends it to the organizer O .

2) Verification and signing. O uses the NIZK. Verify algorithm to verify the validity of π . If verification fails, O outputs $\perp$ and terminates the protocol. If verification succeeds, O executes the signing algorithm of CTS to generate a signature σ and returns σ to U .

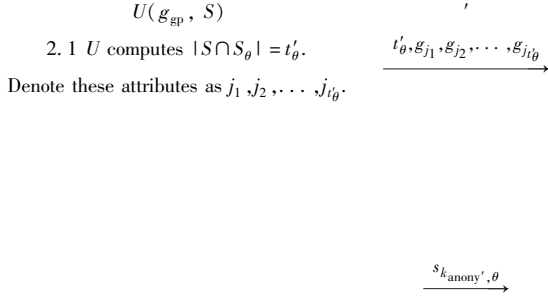
3) Randomization. U executes the CTS. Randomize algorithm to randomize comm into comm' and uses the NIZK. Prove algorithm to generate a new proof π' for comm' .

4) Final verification. For the set of authorities $\{A_{A_\theta}\}_{\theta \in [1, N]}$, execute the CTS. Verify algorithm to verify comm' and run the NIZK. Verify algorithm to

verify π' .

Phase 4 Anonymous key generation

Let the set of attributes of user U be $S = \{j_1, j_2, \dots, j_f\}$ and the random numbers connected to this set be $g_{j_1}, g_{j_2}, \dots, g_{j_f}$. For authorities $\{A_{A_\theta}\}_{\theta \in [1, N]}$, compute $|S \cap S_\theta| = t'_\theta$ and compare t'_θ with t_θ . If $t'_\theta \geq t_\theta$



t_θ , pick the random number $g_{j_1}, g_{j_2}, \dots, g_{j_{t'_\theta}}$ associated with these attributes and compute $r_{anony', \theta}$. Compute the secret key $s_{k_{anony', \theta}} = \mathbf{u}_{anony', \theta} = \mathbf{A}_\theta^{-1}(\mathbf{p}_\theta + \mathbf{B}_\theta \mathbf{r}_{anony', \theta})$. If $t'_\theta < t_\theta$, The calculation of $r_{anony', \theta}$ is different, the rest of the steps are the same. Details of the calculations are shown in Fig. 4.

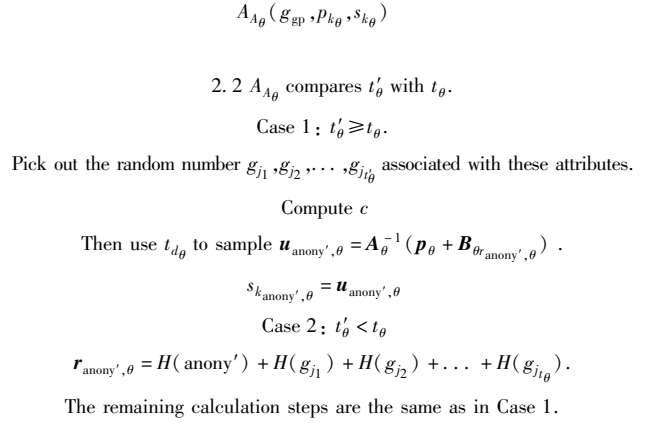


Fig. 4 Anonymous key generation

Note: The private key generation method of this scheme is to generate a common public key for the attributes in the intersection of user attributes and authority-managed attribute collections. Based on the commitment algorithm of Ref. [42] and the techniques of Ref. [38], our scheme can be naturally extended to the protection of attributes.

Phase 5 Encryption stage

The data owner DO selects the message μ to be encrypted, random vectors $s_\theta \leftarrow_R Z_q^n$, $\mathbf{e}_{1, \theta} \leftarrow D_{Z_{\chi}}^n$, $\mathbf{e}_2 \leftarrow D_{Z_{\chi}}^m$, and $\mathbf{e}_3 \leftarrow D_{Z_{\chi}}$. The ciphertext is computed as follows:

$$\mathbf{c}_{1, \theta}^T = s_\theta^T \mathbf{A}_\theta + \mathbf{e}_{1, \theta}^T \quad (3)$$

$$\mathbf{c}_2 = \sum_{\theta \in [1, N]} s_\theta^T \mathbf{B}_\theta + \mathbf{e}_2^T \quad (4)$$

$$\mathbf{c}_3 = \sum_{\theta \in [1, N]} s_\theta^T \mathbf{p}_\theta + \mathbf{e}_3 + \mu \cdot \lfloor q/2 \rfloor \quad (5)$$

The final ciphertext is $c_{\text{ct}} = (\{\mathbf{c}_{1, \theta}^T\}_{\theta \in [1, N]}, \mathbf{c}_2, \mathbf{c}_3)$. After the ciphertext is generated, DO uploads the ciphertext to the cloud server.

Phase 6 Decryption stage

The data user downloads the ciphertext from the cloud, calculate:

$$\left\lceil \frac{2}{q} \left(c_3 + \mathbf{c}_2^T \mathbf{r}_{\text{GID}, \theta} - \sum_{\theta \in [1, N]} \mathbf{c}_{1, \theta}^T \mathbf{u}_{\text{GID}, \theta} \right) \bmod q \right\rceil \quad (6)$$

where

$$\mathbf{c}_{1, \theta}^T \mathbf{u}_{\text{GID}, \theta} = (s_\theta^T \mathbf{A}_\theta + \mathbf{e}_{1, \theta}^T) \mathbf{u}_{\text{GID}, \theta} = s_\theta^T \mathbf{p}_\theta + s_\theta^T \mathbf{B}_\theta \mathbf{r}_{\text{GID}, \theta} + \mathbf{e}_{1, \theta}^T \mathbf{u}_{\text{GID}, \theta} \quad (7)$$

$$\begin{aligned} c_3 + \mathbf{c}_2^T \mathbf{r}_{\text{GID}, \theta} - \sum_{\theta \in [1, N]} \mathbf{c}_{1, \theta}^T \mathbf{u}_{\text{GID}, \theta} &= \sum_{\theta \in [1, N]} s_\theta^T \mathbf{p}_\theta + \mathbf{e}_3 + \\ &\mu \cdot \lfloor q/2 \rfloor + \sum_{\theta \in [1, N]} s_\theta^T \mathbf{B}_\theta \mathbf{r}_{\text{GID}, \theta} + \mathbf{e}_2^T \mathbf{r}_{\text{GID}, \theta} - \\ &\sum_{\theta \in [1, N]} (s_\theta^T \mathbf{p}_\theta + s_\theta^T \mathbf{B}_\theta \mathbf{r}_{\text{GID}, \theta} + \mathbf{e}_{1, \theta}^T \mathbf{u}_{\text{GID}, \theta}) = \\ &\mathbf{e}_3 + \mathbf{e}_2^T \mathbf{r}_{\text{GID}, \theta} + \mu \cdot \lfloor q/2 \rfloor - \sum_{\theta \in [1, N]} \mathbf{e}_{1, \theta}^T \mathbf{u}_{\text{GID}, \theta} \end{aligned} \quad (8)$$

If the error $\| \mathbf{e}_3 + \mathbf{e}_2^T \mathbf{r} - \sum_{\theta \in [1, N]} \mathbf{e}_{1, \theta}^T \mathbf{u}_{\text{GID}, \theta} \| < (q - 1)/4$, then $C = \mu$. Otherwise, the output is $\perp$.

Correctness

Assuming that the conditions of Theorem 3 and Lemma 5, $m \geq m_0(n, q) = O(n \ln q)$, $\chi > \chi_0(n, q) = \sqrt{n \ln q} \cdot w(\sqrt{\ln n})$ hold, then there exists $q_0 = O(M\lambda\chi^2 + \sqrt{\lambda}^{\tau+1} m^\tau \chi_{\text{PRF}\chi}^\tau)$ such that for all $m > m_0$, $q > q_0$, $\chi > \chi_0$, the above construction is correct.

Noise analysis

1) $\| \mathbf{e}_{1, \theta}^T \mathbf{u}_\theta \| \leq \lambda \chi^2$. Let $\psi_1 = (\mathbf{A}_\theta, \mathbf{x}, \mathbf{y})$, where

$A_{\theta} \leftarrow_R Z_q^{n \times m} \mathbf{x} \leftarrow D_{Z, \chi}^m$. $\psi_2 = (A_{\theta}, A_{\theta}^{-1}(\mathbf{p}_{\theta} + B_{\theta} \mathbf{r}), \mathbf{p}_{\theta} + B_{\theta} \mathbf{r})$, where $\mathbf{p}_{\theta} + B_{\theta} \mathbf{r} \leftarrow_R Z_q^n$. Since $\mathbf{p}_{\theta}$ is independent of $B_{\theta} \mathbf{r}$, $\psi_1 \approx_c \psi_2$. Therefore, $\mathbf{u} = A_{\theta}^{-1}(\mathbf{p}_{\theta} + B_{\theta} \mathbf{r}) \approx_c \mathbf{x} \leftarrow D_{Z, \chi}^m$. Based on Fact 4, $\|\mathbf{u}\| \leq \sqrt{\lambda} \chi$. $\mathbf{e}_{1, \theta} \leftarrow D_{Z, \chi}^m$, $\|\mathbf{e}_{1, \theta}\| \leq \sqrt{\lambda} \chi$ based on Fact 4. Therefore, $\|\mathbf{e}_{1, \theta}^T \mathbf{u}_{\theta}\| \leq \lambda \chi^2$.

2) $\|\mathbf{e}_2^T \mathbf{r}\| \leq \sqrt{\lambda}^{I+1} m^I \chi_{\text{PRF}}^I \chi$. According to the construction, $\mathbf{r} = (\prod_{i \in I} (K_i)) \cdot \boldsymbol{\varepsilon}$, $K_i \leftarrow D_{Z, \chi_{\text{PRF}}}^{m \times m}$. Let $K_i = [b_1 | b_2 | \dots | b_m]$, $b_i \leftarrow D_{Z, \chi_{\text{PRF}}}^m$. For $b_i \leftarrow D_{Z, \chi_{\text{PRF}}}^m$, $\|b_i\| \leq \sqrt{\lambda} \chi_{\text{PRF}}$ based on Fact 4. Therefore, $\|K_i\| \leq \sqrt{\lambda} \chi_{\text{PRF}} m$, $\|\mathbf{r}\| \leq \left\| \prod_{i \in I} K_i \right\| \|\boldsymbol{\varepsilon}\| \leq (\sqrt{\lambda} \chi_{\text{PRF}} m)^I$, $\mathbf{e}_2 \leftarrow D_{Z, \chi}^m$, $\|\mathbf{e}_2\| \leq \sqrt{\lambda} \chi$ based on Fact 4. Therefore, $\|\mathbf{e}_2^T \mathbf{r}\| \leq \sqrt{\lambda}^{I+1} m^I \chi_{\text{PRF}}^I \chi$.

3) $\mathbf{e}_3 \leftarrow D_{Z, \chi}^m$, $\|\mathbf{e}_3\| \leq \sqrt{\lambda} \chi$ based on Fact 4.

The total noise $\|\mathbf{e}_{1, \theta}^T \mathbf{u}_{\theta}\| + \|\mathbf{e}_2^T \mathbf{r}\| + \|\mathbf{e}_3\| \leq \lambda \chi^2 + \sqrt{\lambda}^{\tau+1} m^{\tau} c_{\text{chi}}^{\tau} \chi + \sqrt{\lambda} \chi = O(M \lambda \chi^2 + \sqrt{\lambda}^{\tau+1} m^{\tau} \chi_{\text{PRF}}^{\tau} \chi)$. If the error $\|\mathbf{e}_3 + \mathbf{e}_2^T \mathbf{r} - \sum_{\theta \in [1, N]} \mathbf{e}_{1, \theta}^T \mathbf{u}_{\theta}\| < (q-1)/4$, then the ciphertext can be decrypted successfully.

6 Security analysis

6.1 Security proof

Theorem 8 Under the condition of $\text{LWE}(n, m', q, \chi_{\text{PRF}})$ assumption and the e-LWE (n, m, q, χ) assumption, where the parameter $m' = \text{poly}(m, I, Q)$ and Q is an upper bound on the number of secret key queries performed by adversary $\mathcal{A}$, with the noise parameter $\chi > l \lambda^{I+\omega(1)} (m \chi_{\text{PRF}})^{I+1}$, our construction is IND-sAtt-CPA secure.

The security of the scheme is proved by the following three games.

Game 0 It is a security game where the challenger encrypts μ_0 .

Game 1 Game 1 is the same as Game 0, except some changes are made to the ciphertext.

For ciphertext component $\{\mathbf{c}_{1, \theta}\}_{\theta \in [N]}$, $[N] = \{1, 2, \dots, N\}$ change its distribution. $\mathbf{c}_{1, \theta} \leftarrow_R Z_q^n$.

Finally, the ciphertext is

$$c_{\text{ct}} = (\{\mathbf{c}_{1, \theta}^T\}_{\theta \in [N]}, \mathbf{c}_2, \mathbf{c}_3) \quad (9)$$

Game 2 The challenger executes the IND-sAtt-CPA security game and encrypts the message μ_1 .

Theorem 9 If there exists a probabilistic polynomial-time adversary that can distinguish between Game 0 and Game 1 with a non-negligible advantage ε , then a simulator $\mathcal{B}$ can be constructed in the following way, and $\mathcal{B}$ can solve the e-LWE problem with the same non-negligible advantage $A_{\text{advantage } C}^{\text{post}}(\lambda) = \varepsilon$.

Proof

Let N be the number of authorities in the system. Consider the worst-case scenario for the system to occur: the adversary corrupts $N-1$ authorities in the system, leaving only one honest authority A_{A_N} in the system. Let the set of corrupted authorities in the system be $C_{\text{cor}} = \{A_{A_1}, A_{A_2}, \dots, A_{A_{N-1}}\}$.

e-LWE instance

$\mathcal{B}$ receives the e-LWE challenge instance from his challenger $\mathcal{C}$. $(A_N, Z_{1, N}^T) \in Z_q^{n \times m} \times Z_q^m$, $B \in Z_q^{n \times (m+1)}$, $Z_2^T \in Z_q^{1 \times (m+1)}$, $M_N^T \in Z_q^{1 \times m}$

Init

The adversary $\mathcal{A}$ declares the challenge attribute set $\mathcal{S}^*$. It is required that $\mathcal{S}^*$ can not be managed by authorities in C_{cor} .

Set up

1) $\mathcal{B}$ sets the public parameters as follows.

$Q = \{1, 2, \dots, p\}$ represents the set of user attributes in the system. For the security proof, the set $M = \{p+1, p+2, \dots, p+l\}$ is introduced to represent the default attributes in the system.

2) $\mathcal{B}$ constructs the following sets:

$$Q' = Q \cup M = \{1, 2, \dots, p, p+1, p+2, \dots, p+l\} \quad (10)$$

$$W_{i'} = W_i^* \cup \{p+1, p+2, \dots, p+l+1-t_i^*\} \quad (11)$$

3) $\mathcal{B}$ performs a matrix decomposition of $B \in Z_q^{n \times (m+1)}$ he receives from his challenger. B is decomposed into a $n \times m$ dimensional matrices and a $n \times 1$ dimensional matrices, which are denoted as

$$[B_N^* | p_N^*] \quad (12)$$

Besides, $\mathcal{B}$ sets $A_N = A_N^*$, $B_N = B_N^*$, $p_N = p_N^*$.

Public key simulation

For authority AA_N , simulator $\mathcal{B}$ generates the public key $p_{kN} = (A_N^*, B_N^*, p_N^*)$, where A_N^* is obtained by random sampling $A_N^* \leftarrow_R Z_q^{n \times m}$. In the original scheme, A_N is generated by the TrapGen algorithm. Due to the good sampling property of TrapGen, A_N^* and A_N are indistinguishable.

$B_N^* \leftarrow_R Z_q^{n \times m}$ is indistinguishable from $B_N \leftarrow_R Z_q^{n \times m}$ in original scheme.

p_N^* is generated by the decomposition of the matrix $B \leftarrow_R Z_q^{n \times (m+1)}$, consistent with the distribution of p_N in the original scheme.

For $\theta \in [1, N-1]$, $p_{k\theta}$ are generated in the same way as AuthSetup algorithm. The simulator $\mathcal{B}$ sends all $\{p_{k\theta}\}_{\theta \in [1, N]}$ to the adversary $\mathcal{A}$. Due to the indistinguishability of the above public key construction method from the original scheme public key generation, the simulated public key is indistinguishable to adversary $\mathcal{A}$.

Phase 1

The simulator $\mathcal{B}$ reacts to the adversary's private key queries.

Case 1: if the set $\mathcal{S}^* \subseteq Q$ for which the adversary performs private key queries satisfy the access policy $\{t_N, W_N\}$, $\mathcal{B}$ returns $\perp$.

Case 2: if the set $\mathcal{S}^* \subseteq Q$ cannot satisfy the access policy $\{t_N, W_N\}$, i. e., $|\mathcal{S}^* \cap W_N| \leq t_N - 1$. For authority N , the simulator $\mathcal{B}$ constructs $\mathcal{S}$, $W_{N'}$, where $\mathcal{S} = \mathcal{S}^* \cup \{p+1, p+2, \dots, p+l\}$, $W_{N'} = W_N^* \cup \{p+1, p+2, \dots, p+l-1-t_N\}$. Then for A_N , $\mathcal{S} \cap W_{N'} \leq l$. A set $\bar{\mathcal{A}} = l$ can be selected, which satisfies $(\mathcal{S} \cap W_{N'}) \subseteq \bar{\mathcal{A}} \subseteq \mathcal{S}$.

Secret key simulation

Simulator $\mathcal{B}$ generates the decryption key $s_{k_{\text{GID}, N}} = M_{\bar{\mathcal{S}}}$, where $M_{\bar{\mathcal{S}}}$ comes from matrix M_N^T in the challenge instance. In the e-LWE parameter setting, $M_N^* = A_N^{*-1} P_N^*$, where $P_N^* = [p_N^* + B_N^*(H(\text{GID}) + H(\bar{\mathcal{S}}))]$ (13)

This is the same as the distribution of secret keys in the original scheme. For $\theta \in [1, N-1]$, $\{s_{k\theta}\}_{\theta \in [1, N-1]}$ are generated by invoking anonymous key generation algorithm. Therefore, the secret keys in

$\bar{\mathcal{S}}$ are consistent with the original scheme.

Challenge

$\mathcal{A}$ outputs the challenge messages μ_0 and μ_1 with the same length. $\mathcal{B}$ selects $b \in \{0, 1\}$ randomly, and calculates the ciphertext as follows.

Ciphertext simulation

For $\theta \in [1, N-1]$, $c_{1,\theta} = s_\theta^T A_\theta + e_{1,\theta}^T$, where $e_{1,\theta} \leftarrow D_{Z_X}^m$.

For $\theta = N$, $c_{1,N} = z_{1,N}^T$, which comes from the e-LWE instance.

$$c_2 = \sum_{\theta \in [1, N-1]} s_\theta^T B_\theta + \hat{z}_2^T \quad (14)$$

$$c_3 = \sum_{\theta \in [1, N-1]} s_\theta^T p_{\theta^*} + \mu_b \cdot [q/2] + z_3 \quad (15)$$

The final form of challenge ciphertext is $c_i = \{\{c_{1,\theta}^T\}_{\theta \in [N]}, c_2, c_3\}$. $\mathcal{B}$ sends c_i to $\mathcal{A}$ as the challenge ciphertext.

Guess

Upon receiving the guess b' from the adversary $\mathcal{A}$, the simulator $\mathcal{B}$ sends b' to the challenger $\mathcal{C}$ as its guess.

1) $z_{1,N}^T$ and z_2^T are drawn from a pseudorandom distribution, i. e., $z_{1,N}^T = s_N^T A_N + e_{1,N}^T$, where $s_N \leftarrow_R Z_q^n$, $e_{1,N} \leftarrow D_{Z_X}^m$; $z_2^T = s_N^T B_N + e_2^T$, where $e_2 \leftarrow D_{Z_X}^{m+1}$. $z_3 = s_N^T p_N + e_3, e_3 \leftarrow Z_q$.

Let $s^T = [s_1^T \dots s_N^T]$, $e_2^T = [\hat{e} | e_3]$, $\hat{e}_2 \leftarrow Z_q^m, e_3 \leftarrow Z_q$. $c_{1,\theta}^T = z_{1,\theta}^T = s_\theta^T A_\theta + e_{1,\theta}^T, \theta \in [N]$, $z_2^T = [\hat{z}_2 | z_3] = s_N^T B + e_2^T = [s_N^T B_N^* + \hat{e} | s_N^T p_N^* + e_3]$ (16)

The challenge ciphertext constructed in this way are

$$c_{1,\theta}^T = s_\theta^T A_\theta + e_{1,\theta}^T \quad (17)$$

$$c_{2,\theta} = \sum_{\theta \in [N]} s_\theta^T B_\theta + \hat{e}_2 \quad (18)$$

$$c_{3,\theta} = \sum_{\theta \in [N]} s_\theta^T p_\theta + \mu_0 \cdot [q/2] + e_3 \quad (19)$$

The distribution of the challenge ciphertext is identical to the ciphertext distribution in Game 0.

2) $z_{1,N}^T$ and z_2^T are uniformly distributed over $Z_q^m \times Z_q^{m+1}$, for the authority A_N , the ciphertext $z_{1,N} \leftarrow_R Z_q^m$, $\hat{z}_2 \leftarrow_R Z_q^{m+1}$ imply that $c_{1,N} \leftarrow_R Z_q^m$. The ciphertext $c_{1,N}$, $c_{2,N}$ and $c_{3,N}$ are also independently and uniformly distributed over $Z_q^m \times Z_q^m \times Z_q$. The distribution of the ciphertext is identical to that in Game 1.

Therefore, $\mathcal{B}$ can utilize $\mathcal{A}$ to distinguish which distribution its obtained e-LWE instance originates

from.

In summary, if the adversary $\mathcal{A}$ can differentiate between Game 0 and Game 1 with non-negligible advantage ε , then the simulator $\mathcal{B}$ can break the e-LWE assumption with the same advantage $A_{\text{advantage } \mathcal{C}}^{\text{post}}(\lambda) = \varepsilon$. According to Ref. [23], $A_{\text{advantage } \mathcal{A}}^{\text{pre}}(\lambda)$ is negligible, hence it is omitted in the proof of this scheme. Based on the relationship between $A_{\text{advantage } \mathcal{A}}^{\text{pre}}(\lambda)$ and $A_{\text{advantage } \mathcal{A}}^{\text{post}}(\lambda)$ defined in Assumption 2, the advantage $A_{\text{advantage } \mathcal{A}}^{\text{post}}(\lambda)$ is also negligible. Consequently, the adversary $\mathcal{A}$ can only distinguish Game 0 and Game 1 with a negligible advantage. Furthermore, under the e-LWE assumption, it can be shown by a similar argument that Game 1 and Game 2 are computationally indistinguishable for adversary $\mathcal{A}$. Thus, the proposed scheme achieves IND-sAtt-CPA security.

According to Ref. [23], $A_{\text{advantage } \mathcal{B}_0}^{\text{pre}} = g_{\text{negligible0}}(\lambda)$.

By applying the formula from Assumption 2,

$$\begin{aligned} & \frac{A_{\text{advantage } \mathcal{B}}^{\text{post}}}{\text{poly}(\lambda)} - g_{\text{negligible1}}(\lambda) \leq g_{\text{negligible0}}(\lambda) A_{\text{advantage } \mathcal{B}}^{\text{post}} \leq \\ & \text{poly}(\lambda) \cdot (g_{\text{negligible0}}(\lambda) + g_{\text{negligible1}}(\lambda)) \cdot \\ & A_{\text{advantage } \mathcal{A}}^{\text{IND-sAtt-CPA}}(\lambda) = \\ & |\Pr[\text{Game}_0^{\mathcal{A}} = 1] - \Pr[\text{Game}_2^{\mathcal{A}} = 1]| \leq \\ & |\Pr[\text{Game}_0^{\mathcal{A}} = 1] - \Pr[\text{Game}_1^{\mathcal{A}} = 1]| + \\ & |\Pr[\text{Game}_1^{\mathcal{A}} = 1] - \Pr[\text{Game}_2^{\mathcal{A}} = 1]| \leq \\ & A_{\text{advantage } \mathcal{B}}^{\text{post}}(\lambda) + g_{\text{negligible}'}(\lambda) + A_{\text{advantage } \mathcal{B}}^{\text{post}}(\lambda) + \\ & g_{\text{negligible}''}(\lambda) \leq g_{\text{negligible}}(\lambda) \end{aligned} \quad (20)$$

6.2 Anonymity analysis

Here we demonstrate the anonymity of our scheme.

1) Bilateral anonymity

During registration, U sends comm and NIZK proof π instead of its GID. The Baum-Damgård-Lyubashevsky-Oechsner-Peikert (BDLOP) commitment^[42] is hiding under the decisional Knapsack problem (DKS) problem, while NIZK reveals only statement validity; therefore, organization O learns no GID information.

During verification, the Transfer algorithm converts σ to σ' , the Randomize algorithm converts comm to comm', and NIZK proves their validity. By CTS simulatability^[38], NIZK zero knowledge, and

commitment hiding, verifier V learns no user identity. Thus, the scheme provides both user-to-organization and user-to-verifier anonymity.

2) Unlinkability

Since comm' is independently rerandomized and transferred signatures are simulatable, no probabilistic polynomial-time adversary can determine whether two valid pseudonyms originate from the same user.

3) Unforgeability

Suppose an adversary $\mathcal{A}$ forges a valid credential without obtaining one from O . A simulator $\mathcal{B}$ answers registration queries through NIZK extraction and forwards issuance queries to its CTS signing oracle. A successful credential forgery by $\mathcal{A}$ therefore yields a CTS forgery, contradicting the unforgeability of the CTS scheme.

7 Performance analysis

7.1 Functional comparison

In this section, we compare the functionalities of our proposed scheme with existing schemes of the same category. Table 2 presents a comparative analysis between our scheme and prior works^[14,16,28,23,25,31,42,44] in terms of access structure, support for multi-authority, anonymity, and other critical features. Schemes^[42,44] adopt single-CA architectures, while the others support multiple attribute authorities. Although schemes^[14,16] enable multi-attribute authority frameworks, their CAs remain indirectly involved in distributing attribute keys. Schemes^[25,31] achieve a decentralized multi-attribute authority architecture; however, their constructions rely on bilinear pairings and thus fail to achieve post-quantum security^[28,23], and our scheme support fully decentralized structure where any party can be an authority, and no collaboration between authorities is required except for initializing public parameters. Both the proposed scheme and scheme^[31] incorporate user privacy protection. However, the security of scheme^[31] is based on the BDH assumption, rendering it vulnerable to quantum computing threats.

Table 2 Scheme characteristics

Scheme	Access structure	Multi-authority	Anonymity	Assumption	Resist quantum computing attack
Scheme in Ref. [14]	Threshold	CA + MA	×	LWE	✓
Scheme in Ref. [16]	Threshold	CA + MA	×	Ring learning with errors (RLWE)	✓
Scheme in Ref. [23]	Subset policy	DMA	×	Evasive LWE	✓
Scheme in Ref. [25]	LSSS	DMA	×	Composite order subgroup decision	×
Scheme in Ref. [28]	DNF	DMA	×	LWE	✓
Scheme in Ref. [31]	Access tree	DMA	✓	Bilinear Diffie-Hellman assumption	×
Scheme in Ref. [42]	And“ + ” attributes and “ - ” attributes	CA	×	LWE	✓
Scheme in Ref. [44]	Abstract access policy	CA	×	LWE	✓
The proposed scheme	Threshold	DMA	✓	E-LWE	✓

7.2 System parameter setting

Following the computational steps outlined in Ref. [45] and considering the correctness conditions required for the proposed scheme in this work, we adopted a methodology analogous to Ref. [29] to determine the values of q , n , m , and the security parameter λ , under the Gaussian width parameter $\chi = 8$ and adversarial advantages of 2^{-1} and 2^{-32} . The resulting parameter sets are summarized in Table 3.

Table 3 Parameter set for Gaussian parameter and adversary’s advantage 2^{-1} , 2^{-32}

Parameter	$A_{\text{Advantage}} = 2^{-1}$			$A_{\text{Advantage}} = 2^{-32}$		
$\text{lb } q$	42	80	92	42	80	92
λ	75	128	256	75	128	256
n	874	2 371	4 258	826	2 199	4 122
m	36 708	189 680	391 736	34 692	175 920	379 224

7.3 Storage overhead

A comparative analysis between the proposed scheme and existing work regarding public key, secret key and ciphertext sizes is provided in this section, with full comparisons listed in Table 4.

Table 4 Storage cost comparison

Scheme	Public parameter size	Secret key size	Ciphertext size
Scheme in Ref. [14]	$(mn \mathcal{S} + 2n)\text{lb } q$	$m \mathcal{S} \text{lb } q$	$1 + \mathcal{P} + \mathcal{AU} \text{mlb } q$
Scheme in Ref. [23]	$(2mn + n) \mathcal{S} \text{lb } q$	$m \mathcal{S} \text{lb } q$	$m(\mathcal{S} + 1)\text{lb } q + 1$
Scheme in Ref. [28]	$2mn \mathcal{S} \text{lb } q$	$2m \mathcal{U} \text{lb } q$	$(2 \mathcal{P} + 1)\text{mlb } q$
Scheme in Ref. [42]	$(mn + 2mn \mathcal{S} + n)\text{lb } q$	$(1 + \mathcal{S})\text{lb } q$	$(m - 2mR - m \mathcal{P})\text{lb } q + 1$
Scheme in Ref. [44]	$(l + 4)mn\text{lb } q$	$(4m^2 + 2m^2\text{lb } N)\text{lb } q$	$(l + 7)\text{mlb } q$
The proposed scheme	$(2mn + n) \mathcal{AU} \text{lb } q$	$m \mathcal{AU} \text{lb } q$	$m(\mathcal{AU} + 1)\text{lb } q + 1$

Symbols are defined as follows, $|\mathcal{S}|$ for the full set of attributes, $|\mathcal{AU}|$ for the number of authorities, $|\mathcal{U}|$ for the number of attributes owned by the user, $|\mathcal{P}|$ for the number of attributes in the access policy, and N for the number of users in the system. In Ref. [46], l represents the attribute dimension. The proposed scheme yields a smaller public key size than competing constructions. In practical settings where the number of attribute authorities is far lower than the total attributes within the universal set, superior secret key efficiency can be attained. Ciphertext size is comparable to that of similar schemes, scaling as $O(N\text{lb } q)$. The exact size depends on the attribute dimension l , the number of authorities $|\mathcal{AU}|$, and the number of attributes specified in the access policy $|\mathcal{P}|$.

The adopted evaluation methodologies similar to those in Refs. [15,17,29] to analyze the performance of our scheme. As our proposal is constructed on the evasive-LWE, we specifically compare its storage and computational costs with scheme^[23], which is also based on e-LWE.

Table 5 presents a storage cost comparison under the parameter settings $\lambda = 75$, $n = 874$, $m = 36\ 708$, $\text{lb } q = 42$, $|\mathcal{S}| = 6$, $|\mathcal{AB}| = 3$. As shown in Table 5, our scheme exhibits significantly lower storage overhead compared to scheme^[23]. This disparity arises because scheme in Ref. [23] suffers from the “one-authority-per-attribute” design limitation, which inherently increases both storage and computational costs.

Table 5 Comparison of storage overhead

Scheme	Public key	Secret key	Ciphertext
	size/kB	size/kB	size/kB
Scheme in Ref. [22]	1 927.61	1.102 7	1.286 5
The proposed scheme	963.80	0.551 4	0.735 2

Although our public key storage remains relatively large, this can be mitigated in practical applications by leveraging public key compression techniques from Kyber^[46]. Furthermore, our scheme achieves lower time overhead than scheme^[23].

7.4 Implementation and assessment

Adopting methodologies presented in Refs. [15,17,

29], the construction is deployed on the Ubuntu 18.04 operating system. Performance evaluation of the scheme is conducted on hardware equipped with an Intel (R) Core (TM) i5-8250U CPU running at 1.60 GHz. The scheme relies on e-LWE, a variant of the LWE hardness assumption. According to the security proof in Ref. [23], the scheme supports extension to ring-oriented implementations. Scheme simulation leverages Palisade Library v1.11.9, whose underlying cryptographic design adopts RLWE. All metrics are averaged over 20 independent trials.

Under the given parameter settings $\lambda = 75$, $n = 874$, $m = 36\ 708$, $\text{lb } q = 42$, the encryption and key generation runtime of the presented scheme is contrasted against the scheme in Ref. [23], with visualized outcomes provided in Table 6. The experimental setup initializes the system with three attribute authorities where each authority administers a single attribute. In the construction of Ref. [23], every authority controls only one attribute. Accordingly, the total quantity of authorities rises linearly alongside attribute count, which yields a linear increase in the invocation time of the trapdoor generation algorithm. For the above reasons, the presented scheme achieves superior performance on encryption and key generation compared with Ref. [23].

Table 6 Comparison of key generation and encryption time with different numbers of attributes

Scheme	Time required for key generation/ms				Time required for encryption/ μ s			
	3	6	9	12	3	6	9	12
Scheme in Ref. [22]	105.17	210.35	315.52	420.69	629.76	1 259.52	1 889.28	2 519.04
The proposed scheme	105.17	107.10	109.25	111.30	629.76	636.00	641.33	646.76

8 Conclusions

In this paper, a privacy-preserving personal health record sharing system based on decentralized key-policy attribute-based encryption is presented. Commitment signature technology, CTS transfer techniques^[38], and zero-knowledge proofs are employed jointly to achieve user anonymity. This

scheme can solve the problem of the authority collecting the user’s attributes by tracking the user’s GID and thus impersonating the user. Unlike lattice-based blind signatures and group signatures, which only guarantee the user privacy toward the certifying or verifying party, this scheme can achieve bilateral privacy protection for the user. The one-authority-per-attribute management in current decentralized solutions is also extended to multi-attribute management.

Therefore, compared with existing schemes, this scheme not only enables decentralized management but also provides stronger user privacy protection, which is suitable for distributed management and enhances the usability of the PHR-data sharing platform. The proposed scheme exhibits efficiency and has been demonstrated to achieve IND-sAtt-CPA security under the e-LWE assumption.

Follow-up research will target richer expressiveness for the construction's access structures, more generic access policies, and stronger user privacy protection. Additional efficiency optimizations for the construction are also being explored.

References

- [1] SAHAI A, WATERS B. Fuzzy identity-based encryption. *Advances in Cryptology: Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'05)*, 2005, May 22 – 26, Aarhus, Denmark. Berlin, Germany: Springer, 2005: 457 – 473.
- [2] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for finegrained access control of encrypted data. *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS'06)*, 2006, Oct 30 – Nov 3, Alexandria, VA, USA. New York, NY, USA: ACM, 2006: 89 – 98.
- [3] WANG H Y, LIANG J L, DING Y, et al. Ciphertext-policy attribute-based encryption supporting policy-hiding and cloud auditing in smart health. *Computer Standards & Interfaces*, 2023, 84: Article 103696.
- [4] ZHANG L Y, YOU W T, MU Y. Secure outsourced attribute-based sharing framework for lightweight devices in smart health systems. *IEEE Transactions on Services Computing*, 2021, 15(5): 3019 – 3030.
- [5] ZHONG H, ZHOU Y Y, ZHANG Q Y, et al. An efficient and outsourcing-supported attribute-based access control scheme for edge-enabled smart healthcare. *Future Generation Computer Systems*, 2021, 115: 486 – 496.
- [6] SU J, ZHANG L Y, MU Y. BA-RMKABSE: Blockchain-aided ranked multikeyword attribute-based searchable encryption with hiding policy for smart health system. *Future Generation Computer Systems*, 2022, 132: 299 – 309.
- [7] SHOR P W. Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 1994, Nov 20 – 22, Santa Fe, NM, USA. Piscataway, NJ, USA: IEEE, 1994: 124 – 134.
- [8] GROVER L K. A fast quantum mechanical algorithm for database search. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC'96)*, 1996, May 22 – 24, Philadelphia, PA, USA. New York, NY, USA: ACM, 1996: 212 – 219.
- [9] FORD P. The quantum cybersecurity threat may arrive sooner than you think. *Computer*, 2023, 56(2): 134 – 136.
- [10] MICCIANCIO D. Lattice-based cryptography. VAN TILBORG H C A, JAJODIA S (eds). *Encyclopedia of Cryptography and Security*, 2nd edn. Berlin, Germany: Springer, 2011: 347 – 349.
- [11] ZHAO S Y, JIANG R, BHARGAVA B. RL-ABE: A revocable lattice attribute-based encryption scheme based on R-LWE problem in cloud storage. *IEEE Transactions on Services Computing*, 2022, 15(2): 1026 – 1035.
- [12] ZHANG Y H, LIU X M, HU Y P. Simplified server-aided revocable identity-based encryption from lattices. *Provable and Practical Security: Proceedings of the 16th International Conference on Provable and Practical Security (ProvSec'22)*, 2022, Nov 11 – 12, Nanjing, China. Berlin, Germany: Springer, 2022: 71 – 87.
- [13] CHEN E, ZHU Y, LIANG K T, et al. Secure remote cloud file sharing with attribute-based access control and performance optimization. *IEEE Transactions on Cloud Computing*, 2023, 11(1): 579 – 594.
- [14] ZHANG G Y, QIN J, QAZI S. Multi-authority attribute-based encryption scheme from lattices. *Journal of Universal Computer Science*, 2015, 21(3): 483 – 501.
- [15] HUANG B X, GAO J T, LI X L. Efficient lattice-based revocable attribute-based encryption against decryption key exposure for cloud file sharing. *Journal of Cloud Computing*, 2023, 12: Article 37.
- [16] LIU Z C, JIANG Z L, WANG X, et al. Multi-authority ciphertext policy attribute-based encryption scheme on ideal lattices. *Proceedings of the 2018 IEEE International Conference on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom'18)*, 2018, Dec 11 – 13, Melbourne, Australia. Piscataway, NJ, USA: IEEE, 2018: 1003 – 1008.
- [17] YANG Y, SUN J G, LIU Z C, et al. Practical revocable and multi-authority CP-ABE scheme from RLWE for Cloud Computing. *Journal of Information Security and Applications*, 2022, 65: Article 103108.
- [18] XIE S W, ZHANG L Y, WU Q, et al. Flexibly expressive and revocable multi-authority KP-ABE scheme from RLWE for Internet of medical things. *Journal of Systems Architecture*, 2024, 152: Article 103179.
- [19] ZHANG Y H, LIU X M, HU Y P, et al. An improved group signature scheme with VLR over lattices. *Security and Communication Networks*, 2021; DOI: 10.1155/2021/9988939.
- [20] SUN Y R, LIU Y Y. An efficient fully dynamic group signature with message dependent opening from lattice. *Cybersecurity*, 2021, 4: Article 15.
- [21] AGRAWAL S, KIRSHANOVA E, STEHLÉ D, et al. Practical, round-optimal lattice-based blind signatures. *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS'22)*, 2022, Nov 7 – 11, Los Angeles, CA, USA. New York, NY, USA: ACM, 2022: 39 – 53.
- [22] LI C Y, TIAN Y, CHEN X B, et al. An efficient anti-quantum lattice-based blind signature for blockchain-enabled systems.

- Information Sciences, 2021, 546: 253 – 64.
- [23] WATERS B, WEE H, WU D J. Multi-authority ABE from lattices without random oracles. *Theory of Cryptography: Proceedings of the 20th International Conference on Theory of Cryptograph (TCC'22)*, 2022, Nov 7 – 10, Chicago, IL, USA. Cham, Switzerland: Springer Nature Switzerland, 2022: 651 – 679.
 - [24] CHASE M. Multi-authority attribute based encryption. *Theory of Cryptography: Proceedings of the 4th Conference on Theory of Cryptograph (TCC'07)*, 2007, Feb 21 – 24, Amsterdam, The Netherlands. Berlin, Germany: Springer, 2007: 515 – 534.
 - [25] LEWKO A, WATERS B. Decentralizing attribute-based encryption. *Advances in Cryptology: Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Technique (EUROCRYPT'11)*, 2011, May 15 – 19, Tallinn, Estonia. Berlin, Germany: Springer, 2011: 568 – 588.
 - [26] LIU Y, WANG L C, LI L X, et al. Secure and efficient multi-authority attribute-based encryption scheme from lattices. *IEEE Access*, 2018, 7: 3665 – 3674.
 - [27] WANG Z D, FAN X, LIU F H. FE for inner products and its application to decentralized ABE. *Proceedings of the 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC'19)*, 2019, Apr 14 – 17, Beijing, China. Berlin, Germany: Springer, 2019: 97 – 127.
 - [28] DATTA P, KOMARGODSKI I, WATERS B. Decentralized multi-authority ABE for DNFs from LWE. *Advances in Cryptology: Proceedings of the 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'21)*, 2021, Oct 17 – 21, Zagreb, Croatia. Berlin, Germany: Springer, 2021: 177 – 209.
 - [29] YAO Y F, CHEN H Y, GAO Y, et al. A decentralized multi-authority CP-ABE scheme from LWE. *Journal of Information Security and Applications*, 2024, 82: Article 103752.
 - [30] CHASE M, CHOW S S. Improving privacy and security in multi-authority attribute-based encryption. *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS'09)*, 2009, Nov 9 – 13, Chicago, IL, USA. New York, NY, USA: ACM, 2009: 121 – 130.
 - [31] HAN J G, SUSILO W, MU Y. Privacy-preserving decentralized key-policy attribute-based encryption. *IEEE Transactions on parallel and distributed systems*, 2012, 23(11): 2150 – 2162.
 - [32] QIAN H L, LI J G, ZHANG Y C. Privacy-preserving decentralized ciphertext-policy attribute-based encryption with fully hidden access structure. *Information and Communications Security: Proceedings of the 15th International Conference on Information and Communications Security (ICICS '13)*, 2013, Nov 20 – 22, Beijing, China. Berlin, Germany: Springer, 2013: 363 – 372.
 - [33] HAN J G, SUSILO W, MU Y, et al. Improving privacy and security in decentralized ciphertext-policy attribute-based encryption. *IEEE Transactions on information forensics and security*, 2015, 10(3): 665 – 678.
 - [34] WANG M Q, ZHANG Z F, CHEN C. Security analysis of a privacy-preserving decentralized ciphertext-policy attribute-based encryption scheme. *Concurrency and Computation: Practice and Experience*, 2016, 28(4): 1237 – 1245.
 - [35] ZHOU Y W, XU R, QIAO Z R, et al. An anonymous and efficient multimessage and multireceiver certificateless signcryption scheme for VANET. *IEEE Internet of Things Journal*, 2023, 10(24): 22823 – 22835.
 - [36] JEUDY C, ROUX-LANGLOIS A, SANDERS O. Lattice signature with efficient protocols, application to anonymous credentials. *Advances in Cryptology: Proceedings of the 43rd International Cryptology on Advances in Cryptology (CRYPTO'23)*, 2023, Aug 20 – 24, Santa Barbara, CA, USA. Berlin, Germany: Springer, 2023: 351 – 383.
 - [37] BOOTLE J, LYUBASHEVSKY V, NGUYEN N K, et al. A framework for practical anonymous credentials from lattices. *Advances in Cryptology: Proceedings of the 43rd International Cryptology on Advances in Cryptology (CRYPTO'23)*, 2023, Aug 20 – 24, Santa Barbara, CA, USA. Berlin, Germany: Springer, 2023: 384 – 417.
 - [38] LAI Q Q, LIU F H, LYSYANSKAYA A, et al. Lattice-based commit-transferrable signatures and applications to anonymous credentials. *IACR Cryptol ePrint Arch*, 2023: Article 766.
 - [39] REGEV O. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 2009, 56(6): 1 – 40.
 - [40] MICCIANCIO D, PEIKERT C. Trapdoors for lattices: Simpler, tighter, faster, smaller. *Advances in Cryptology: Proceedings of the 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'12)*, 2012, Apr 15 – 19, Cambridge, UK. Berlin, Germany: Springer, 2012: 700 – 718.
 - [41] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions. *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, 2008, May 17 – 20, Victoria, Canada. New York, NY, USA: ACM, 2008: 197 – 206.
 - [42] BAUM C, DAMGÅRD I, LYUBASHEVSKY V, et al. More efficient commitments from structured lattice assumptions. *Security and Cryptography for Networks: Proceedings of the 11th International Conference on Security and Cryptography for Networks (SCN'18)*, 2018, Sept 5 – 7, Amalfi, Italy. Berlin, Germany: Springer, 2018: 368 – 385.
 - [43] ZHANG J, ZHANG Z F. A ciphertext policy attribute-based encryption scheme without pairings. *Information Security and Cryptology: Proceedings of the 7th International Conference on Information Security and Cryptology (INSCRYPT'11)*, 2011, Nov 30 – Dec 3, Beijing, China. Berlin, Germany: Springer, 2011: 324 – 340.
 - [44] DONG X T, HU Y P, WANG B C, et al. Lattice-based revocable attribute-based encryption with decryption key exposure resistance. *IET Information Security*, 2021, 15(6): 428 – 441.
 - [45] CHEN Z G, SHI Y F, SONG X X. Fully homomorphic encryption concrete security parameter analysis. *Journal of Cryptology*, 2016, 3(5): 480 – 491. (in Chinese)
 - [46] AVANZI R, BOS J, DUCAS L, et al. CRYSTALS-Kyber algorithm specifications and supporting documentation. *NIST PQC Round*, 2017: 32p.

(Editor: Luo Lang)