entropy

MDPI

Article

Attribute-Based Verifiable Conditional Proxy Re-Encryption Scheme

Yongli Tang, Minglu Jin, Hui Meng *, Li Yang and Chengfu Zheng

College of Software, Henan Polytechnic University, Jiaozuo 454000, China; yltang@hpu.edu.cn (Y.T.)
* Correspondence: menghui@hpu.edu.cn

Abstract: There are mostly semi-honest agents in cloud computing, so agents may perform unreliable calculations during the actual execution process. In this paper, an attribute-based verifiable conditional proxy re-encryption (AB-VCPRE) scheme using a homomorphic signature is proposed to solve the problem that the current attribute-based conditional proxy re-encryption (AB-CPRE) algorithm cannot detect the illegal behavior of the agent. The scheme implements robustness, that is the re-encryption ciphertext, can be verified by the verification server, showing that the received ciphertext is correctly converted by the agent from the original ciphertext, thus, meaning that illegal activities of agents can be effectively detected. In addition, the article demonstrates the reliability of the constructed AB-VCPRE scheme validation in the standard model, and proves that the scheme satisfies CPA security in the selective security model based on the learning with errors (LWE) assumption.

Keywords: proxy re-encryption; homomorphic signature; learning with errors; re-encryption verifiable

1. Introduction

As a new resource sharing in the field of information, cloud computing is constantly changing people's lives. As an important technology in cloud computing, cloud storage is used to organize a series of different types of network storage devices to facilitate data sharing. To ensure the confidentiality of data, before being uploaded to a cloud server, user data are encrypted, however, this poses difficulties in sharing data between different users. When dealing with a significant quantity of data recipients, general encryption algorithms can significantly increase the computational and communication expenses incurred by the data owner. Proxy re-encryption (PRE) effectively solves this problem.

In 1998, Blaze et al. [1] first introduced the concept of PRE at the Euromonitor Conference. PRE is a data cipher conversion in cloud computing, which ensures both user data security and flexible access and sharing of data. However, in the traditional PRE system, it is usually one delegator that corresponds to another delegator, that is, a one-to-one model; this implies that only one client's message can be re-encrypted at a time, necessitating a large amount of communication overhead and computation expense, which is contrary to the initial aim of cloud computing customers wanting to save money. In 2007, GREEN et al. [2] simplified the public key certificate authentication process by proposing an encryption scheme based on user identity information instead of a public key. However, the encryption process is specific to particular users and requires explicit information about the recipient. In 2009, JIAN et al. [3] suggested a strategy for conditional PRE (CPRE) based on identity proxy re-encryption. By designing a conditional ciphertext conversion method, the ciphertext can only be converted when the ciphertext meets the set conditions, enabling the assignment of partial decryption rights, but it is still in the form of a one-to-one assignment between the authorizer and the authorized person, which not only severely restricts users' ability to selectively share data with other users at a fine-grained level, but it also has the problems of high communication costs and high computational overhead when a large number of users need to access that shared data, as well as wasting a large amount of local memory space to hold a large number of decryption keys.

check for updates

Citation: Tang, Y.; Jin, M.; Meng, H.; Yang, L.; Zheng, C. Attribute-Based Verifiable Conditional Proxy Re-Encryption Scheme. *Entropy* **2023**, *25*, 822. https://doi.org/10.3390/e25050822

Academic Editors: Bill William Buchanan, Jawad Ahmad and Arslan Munir

Received: 15 March 2023
Revised: 12 May 2023
Accepted: 18 May 2023
Published: 19 May 2023

Being a novel cryptographic technique that differs from conventional public key cryptography, attribute-based encryption (ABE) [4] is ideally suited for resolving data confidentiality protection and access control of ciphertext problems in cloud storage applications [5]. ABE technology can provide an effective one-to-many, fine-grained ciphertext access control solution for cloud storage data security. AB-CPRE schemes have been presented that demonstrate the advantages and properties of ABE and CPRE. However, the existing AB-PRE schemes and AB-CPRE schemes are mostly based on constructs such as linear mappings or discrete logarithmic puzzles [6,7]. Due to the advent of quantum computers, the security of traditional number theory puzzles is threatened and these schemes will become insecure. To solve this problem, a lattice cipher is proposed. It is believed that lattice-based cryptography can resist quantum attacks and has high computational efficiency. Therefore, lattice-based public key cryptography schemes have attracted wide attention in recent years.

However, all the AB-CPRE schemes [8–10] that are currently in use are semi-trusted agents, so they may perform unreliable calculations, which bring security problems to data sharing. Most AB-CPRE efforts focus on data privacy and access control without considering re-encryption authentication, which can lead to incorrect results for users.

Therefore, it is of interest to ensure that the re-encryption ciphertext is converted correctly from the original ciphertext. In a homomorphic encryption algorithm, the user can perform some kind of secure proxy calculation with the untrusted remote server. In this process, the server cannot see any private information. The homomorphic signature algorithm supports the signature operation consistent with the message, and the generated signature does not disclose any information related to the data set, which can meet the security requirements in the cloud environment, and is very suitable for the sensor network, network coding, and other message operation scenarios to ensure information security. This paper introduces homomorphic signature techniques in AB-CPRE, provides a verification mechanism for re-encryption performed by a verification server, and proposes a verifiable PRE scheme.

Our main contributions in this article are as follows:

- An AB-VCPRE scheme based on LWE is proposed. The scheme ensures by verification that the re-encryption ciphertext is correctly converted from the encryption ciphertext;
- Fine-grained access control is implemented. In combination with fully homomorphic encryption, the delegation policy supports any polynomial-depth boolean circuit;
- Robustness is achieved. The scheme uses a validation algorithm to achieve robustness. Forged or incorrectly shared ciphertexts can be detected by validating the re-encryption ciphertext with a validation server;
- The scheme satisfies CPA security. The ciphertext in our scheme needs to be signed and verified using an unforgeable homomorphic signature. This paper demonstrates that the constructed AB-VCPRE scheme is CPA security based on a LWE problem.

The rest of the paper is organized into seven sections. In Section 2, the related studies are described. In Section 3, the relevant definitions are introduced. In Sections 4 and 5, we state the details of the scheme and the security analysis. Section 6 presents the efficiency analysis. The last section is a summary of the paper.

2. Related Work

Liang et al. [7] present an AB-PRE cryptographic primitive based on the augmented decisional bilinear Diffie–Hellman (DBDH) problem combining ABE and PRE for the first time, which empowers users to authorize in an access control environment. Li et al. [11] propose a proxy re-encryption scheme for a re-splitable threshold multi-agent, which is different from the encryption scheme on the ciphertext input and output plane and the re-encryption surface, which means the noise boundary has a wider range of choices and can ensure the security of the re-encryption key. Nunez et al. [12] propose a typical threshold proxy re-encryption scheme, which is based on a DBDH assumption, vulnerable to quantum attacks. Luo et al. [13] construct a standard lattice multi-hop AB-PRE scheme,

which supports circuit access, has a short key, the key size is dependent on the depth of the circuit policy, and satisfies CPA security requirements based on the LWE problem in the selection security model. However, these PRE schemes may not show sufficient flexibility and practicality when the data owner wishes to select some but not all of the data for dissemination to certain users. Weng et al. [3] proposed a CPRE scheme where only those that satisfy the conditions can be re-encrypted, but it can only be applied to simple keyword-based conditions and will be limited in practical applications. Then, Yang et al. [8] propose a ciphertext policy-based AB-CPRE scheme, which supports a fine-grained decryption delegation. The ciphertext in the scheme is related to the access policy while the re-encryption key is related to the attributes, and the ciphertext can be re-encrypted only when the access policy satisfies the attributes. Huang et al. [14] propose PRECISE, which combines AB-CPRE with IBBE to support fine-grained re-encryption conditions for IBBE ciphertexts. Yao et al. [15] combine ciphertext authorization, key update, and ciphertext evolution to propose an improved revocable, identity-based ciphertext evolution conditional proxy re-encryption scheme for secure and efficient cloud data sharing.

The universal CPRE algorithm cannot ensure the cloud server's integrity during the re-encryption procedure, while the homomorphic signature algorithm has unforgettable security and privacy, which can effectively verify the honesty of the proxy during the re-encryption. Therefore, this paper uses a homomorphic signature algorithm to propose a PRE scheme with encryption validating on the lattice, which can effectively detect the illegal behavior of the proxy and provide a guarantee for the safe sharing of data.

3. Preliminaries

3.1. Lattice

Definition 1 (lattice). *The lattice is a linear combination of group $b_1, b_2, \ldots, b_n$'s linearly independent vectors' $n(m \geq n)$ integer coefficients in m-dimensional Euclidean space R^m, which is defined as:*

$$L(B) = \left\{ \sum_{i=1}^{n} x_i b_i : x_i \in \mathbb{Z}, i = 1, \ldots, n \right\}. \tag{1}$$

Lemma 1 ([16]). *Take integer $q \geq 3$, $m \geq 6n \log q$, $\sigma \geq m^2 \omega\left(\sqrt{\log m}\right)$, there exists a PPT algorithm $TrapGen(1^n, 1^m, q)$ that generates a matrix $A \in \mathbb{Z}_q^{n \times m}$ and a trapdoor $T_A \in \mathbb{Z}^{m \times m}$ for the lattice $\wedge_q^{\perp}(A)$,* i.e., *there is $AT_A = 0 \bmod q$, such that the distribution statistics satisfied by the matrix A are close to a uniform distribution on $\mathbb{Z}_q^{n \times m}$, and $\left|\left|\widetilde{T}_A\right|\right| \leq \mathcal{O}\left(\sqrt{n \log q}\right)$ holds by an absolute margin.*

Lemma 2 ([17]). *Let $q > 2$ and $m > (n+1) \log q + \omega(\log n)$. Select three uniform matrices $D \in \{-1, 1\}^{m \times k}$, $E \in \mathbb{Z}_q^{n \times m}$, and $F \in \mathbb{Z}_q^{n \times k}$ at random for some polynomials with $k = k(n)$. Distribution $\left(E, ED, D^T r\right)$ and $\left(E, F, D^T r\right)$ are statistically indistinguishable for any vector $r \in \mathbb{Z}_q^m$.*

LWE is a difficult problem under lattice. Regev [18] first proposed this in 2005 and proved that the average case is just as difficult to solve for several standard cells.

Definition 2 (LWE). *Given positive integer n, integer $m \geq n$ and $q \geq 2$, choosing uniform random matrix $A \in \mathbb{Z}_q^{n \times m}$ and vector $s \in \mathbb{Z}_q^n$, vector $e \leftarrow \chi^m$ follows the error distribution. Given $\left(A, A^T s + e\right)$, the LWE problem is to find s with non-negligible probability.*

Definition 3 (Small integer solutions problem, SIS). *Let the defining parameters be β, q is a prime number, given positive integers m and n, select a matrix $A \in \mathbb{Z}_q^{n \times m}$ at random, solve for a non-zero vector of integers $z \in \mathbb{Z}^m \backslash \{0\}$ with $||z|| \leq \beta$. In 1996, Ajtai presented the SIS problem*

in the literature [16]. The homomorphic signature used for robustness in the paper is based on the SIS problem.

3.2. Related Functions and Tools

3.2.1. Functions of Bits and Power2

According to the article [19], decomposing the vector into the form of an inner product can effectively control the error range of the vector. The following describes how to decompose vectors into bit representations.

For any $x \in \mathbb{Z}^N$, let $x = \sum_{i=0}^{g-1} 2^i \cdot x^i \bmod q$, $x_i \in \{0,1\}^N$. Output vector $Bit(x) = (x_0, x_1, \ldots, x_{g-1}) \in \{0,1\}^{1 \times Ng}$, where $g = \lceil \log q \rceil$. For any $y = [y_1|y_2|\ldots|y_\ell] \in \mathbb{Z}^{N \times \ell}$, where y_i is a column vector, output matrix

$$Power2(y) = \begin{bmatrix} y_1 & y_2 & \cdots & y_\ell \\ 2y_1 & 2y_2 & \cdots & 2y_\ell \\ \vdots & \vdots & \ddots & \vdots \\ 2^{g-1}y_1 & 2^{g-1}y_2 & \cdots & 2^{g-1}y_\ell \end{bmatrix} \in \mathbb{Z}_q^{Ng \times \ell}. \tag{2}$$

It can be verified that for any $q \in \mathbb{Z}$, there is $\langle Bit(x), Power2(y) \rangle = \langle x, y \rangle \in \mathbb{Z}_q^{1 \times \ell}$.

3.2.2. Discrete Gaussian Distribution

For integer vectors $c \in \mathbb{Z}^m$, $\sigma > 0$, the discrete Gaussian distribution on the m-dimensional lattice Λ is:

$$D_{\wedge,\sigma,c}(x) = \frac{\rho_{\sigma,c}(x)}{\rho_{\sigma,c}(\wedge)} = \frac{\rho_{\sigma,c}(x)}{\sum_{x \in \wedge} \rho_{\sigma,c}(x)}, \forall x \in \mathbb{Z}^m. \tag{3}$$

Lemma 3 ([17]). *Let $q \geq 2$, B is a matrix over $\mathbb{Z}_q^{n \times m}$ and $m > n$. Let T_B is the base of $\wedge_q^\perp(B)$, $\sigma \geq \left\|\widetilde{T}_B\right\| \omega(\sqrt{\log_2 m})$. For $u \in \mathbb{Z}_q^n$, there are:*

1. *Set the rank of $B \in \mathbb{Z}_q^{n \times m}$ is n, $E \in \mathbb{Z}_q^{n \times m}$, $R \in \{-1,1\}^{m \times m}$, $\sigma \geq \left\|\widetilde{T}_B\right\| \omega(\sqrt{\log_2 m})$. Let $F = (B|BR+E) \in \mathbb{Z}_q^{n \times (2m)}$, PPT algorithms $SampleBasisLeft(B, BR+E, T_B, \sigma)$, where T_B is the base of $\wedge_q^\perp(B)$, output a short base $T_F \in \wedge_q^\perp(F)$ statistical distribution to $\psi_\sigma^{(2m)\times(2m)}$;*
2. *$Sample\mathrm{Pre}(B, T_B, \sigma, u)$: There is trapdoor T_B of lattice $\wedge_q^\perp(B)$, the real number $\sigma \geq \left\|\widetilde{T}_B\right\| \cdot \omega(\sqrt{\log n})$, for any vector $u \in \mathbb{Z}_q^n$, a PPT algorithm $Sample\mathrm{Pre}(B, T_B, \sigma, u)$ capable of generating a vector e from a distribution that is statistically close to $D_{\mathbb{Z}^m,\sigma}(x)$, satisfying $Be = u(\bmod q)$;*
3. *Let the rank of $G \in \mathbb{Z}_q^{n \times m}$ be n, $B \in \mathbb{Z}_q^{n \times m}$, a low-dimensional matrix $S \in \{-1,1\}^{m \times m}$, a trapdoor for the lattice $\wedge_q^\perp(G)$, and $\sigma \geq \left\|\widetilde{T}_E\right\| \cdot \left\|R\right\| \omega(\sqrt{\log_2 m})$. PPT algorithm $SampleBasisRight(B, G, S, T_G, \sigma)$ output a short base $T_{(B|BS+G)} \in \wedge_q^\perp(B|BS+G)$ with a statistical distribution close to $\Psi_\sigma^{(2m)\times(2m)}$.*

3.3. Key Homomorphism

By embedding algorithmic circuits in LWE matrices, Boneh et al. suggested an ABE approach for algorithmic circuits in their paper [20], and the method was used in many LWE-based structures, for example, predicate encryption [21], constraint PRFs [22], watermarks for PRFs [23], etc.

Definition 4. *For any positive integer k, d, a g of depth $\leq d$ boolean circuit, defining families of functions $\mathcal{F}_{k,d} = \left\{g : \{0,1\}^k \to \{0,1\}\right\}$.*

Lemma 4 (Fully homomorphic encryption [20,24]). *Given parameters t, h, k, d, q, χ, where χ is a B-bounded noise distribution, h is a security parameter, $h \geq \lceil t \log q \rceil$. For any matrices $B_1, B_2, \ldots, B_\ell \in \mathbb{Z}_q^{t \times h}$, any boolean circuit $g : \{0,1\}^k \to \{0,1\}$ for any depth$\leq d$, $x \in \{0,1\}^k$, matrix $G \in Z_q^{n \times m}$, vector $s \in \mathbb{Z}_q^t$, $e_i \leftarrow \chi^h$ for $i \in [k]$, if $p_i = (x_i G + B_i)^T s + e_i, \forall i \in [k]$,*

1. *$Eval_{pk}(g, (B_1, \ldots B_k))$: Taking a circuit g, k matrices $\{B_i\}_{i \in [k]}$ as input, outputs a matrix B_g;*
2. *$Eval_{ct}\left(g, \{(x_i, p_i, B_i)\}_{i \in [k]}\right)$: Given a circuit g, k matrices $\{B_i\}_{i \in [k]}$, a vector $x \in \{0,1\}^k$ and k vectors $\{p_1, \ldots, p_k\}$, outputs a vector p_g, satisfying $p_g = \left(B_g + g(x)G\right)^T s + e_g$, where $B_g = Eval_{pk}(g, \{B_1, \ldots, B_k\})$, $\left|\left|e_g\right|\right| \leq B\sqrt{h}(1+h)^d$ with all but negligible probability;*
3. *$Eval_{sim}\left(g, \left\{S_i, x_i^*\right\}_{i \in [k]}, A\right)$: On input a circuit g, a vector $x^* \in \{0,1\}^k$, k matrices $\{S_i\}_{i \in [k]}$, a matrix $A \in \mathbb{Z}_q^{t \times h}$, outputs a matrix S_g satisfying $AS_g - g(x^*) = B_g$, where $\left|\left|S_g\right|\right|_2 \leq 20\sqrt{h}(1+h)^d < (1+h)^{d+1}$ with all but negligible probability.*

3.4. Homomorphic Signature

A homomorphic signature is a valid signature that permits any entity to conduct a sequence of operations on the original message and its signature without the signing private key.

Definition 5 (Homomorphic signature). *The probabilistic polynomial-time algorithm $(KG, Sign, SignEval, Verify)$ is included in the following tuple is the homomorphic signature (HS) scheme:*

1. *$HS.KG(\mathrm{p}, d, N)$: Take a safety parameter p, a circuit depth d, and a message length N as input, output a signature private key hssk and a verification key hsvk;*
2. *$HS.Sign(hssk, M)$: Accept as inputs the message M requiring signature and hssk, output the signature σ;*
3. *$HS.SEval(g, \sigma)$: Take an evaluation circuit $g : \{0,1\}^N \to \{0,1\}$ and signature σ as input, output a homomorphic calculation signature σ^*;*
4. *$HS.Verify(hsvk, y, g, \sigma^*)$: Take hsvk, a message y, a circuit g and a signature σ^*, the verification algorithm either accepts the signature (outputs 1) or rejects it (outputs 0).*

Correctness. On input $p, d, N \in \mathbb{Z}$, $HS.KG(p, d, N) \to (hsvk, hssk)$, $M \in \{0,1\}^N$, $HS.Sign(hssk, M) \to \sigma$, any circuit $g : \{0,1\}^N \to \{0,1\}$ with a depth d, $g(M) \to y$, the equation below holds:

$$\Pr[HS.Verify(hsvk, y, g, HS.SEval(g, \sigma)) = 1] = 1. \tag{4}$$

3.5. Robustness

A key component of the AB-VCPRE design is robustness. The fundamental tenet is that by re-encryption key sharing, an adversary cannot create ciphertext that is falsely obtained yet can be correctly authenticated. The following game $Expt_{\mathcal{A}}^{Rb}$ describes the robustness of the AB-VCPRE scheme.

During the guessing phase, the adversary outputs the appropriate ciphertext CT^* satisfies $Verfy(hsvk, CT^*) = 1$ while *Setup*, *KeyGen query*, Re*KeyGen query*, and Re*Enc query* interact as specified in Definition 6.

The adversary's advantage is characterized as $Adv_{\mathcal{A}}^{Rb} = \Pr\left[Expt_{\mathcal{A}}^{Rb}(\lambda) = 1\right]$.

4. The Model of AB-VCPRE with Re-Encryption Verification

4.1. Scheme Definition

An AB-VCPRE scheme consists of seven algorithms. The specific flow chart is shown in Figure 1. In comparison to the standard AB-VCPRE, a verification method called Re$Enc - Ver$ is added to check for an honest transformation of the ciphertext. The Re$Enc - Ver$

algorithm is publicly verifiable because all that is required are the original ciphertext and the corresponding re-encryption ciphertext.

1. $Setup(n)$: Input security parameter n, output public parameters pp;
2. $KeyGen(pp, \alpha)$: Given pp, output the public/private key pair (pk_α, sk_α) for user α;
3. $Enc(pp, pk_\alpha, \mu, x)$: Taking pp, pk_α, plaintext μ, and an attribute vector x as input, output a related ciphertext CT_α with x;
4. $Dec(pp, sk_\alpha, CT_\alpha)$: Taking pp, sk_α, and CT_α as input, output a message μ;
5. Re$KeyGen\left(pp, sk_\alpha, pk_\beta, f\right)$: Input pp, sk_α of user α, pk_β of user β, and a control policy/function f, returns the re-encryption key $RK_{\alpha, f\to\beta}$ related to f and the corresponding signature, outputs the re-encryption verification key $VK_{\alpha\to\beta}$ from user α to user β;
6. Re$Enc\Big(pp, RK_{\alpha, f\to\beta}, CT_\alpha\Big)$: With pp, pk_α of user α, CT_α associated with x, and $RK_{\alpha, f\to\beta}$ as input. When $f(x) = 0$ remains constant, output the converted ciphertext CT_β, otherwise output $\perp$;
7. Re$Enc - Ver\left(VK_{\alpha\to\beta}, CT_\alpha, CT_\beta\right)$: If the original ciphertext's conversion to the re-encryption ciphertext is performed correctly, the output of the authentication algorithm is valid, otherwise output $\perp$ (invalid ciphertext).

Correctness. In an AB-VCPRE scheme, correctness has the following two requirements:

1. Decryption correctness.

For security parameter n, attribute vectors $x = \{x_i\}_{i\in[l]}$, message $\mu \in \{0,1\}^m$, the equations below hold

$$Dec(pp, sk_\alpha, Enc(pp, pk_\alpha, \mu, x)) = \mu; \tag{5}$$

$$Dec\Big(pp, sk_\beta, \text{Re}Enc\Big(pp, RK_{\alpha, f\to\beta}, CT_\alpha\Big)\Big) = \mu, \tag{6}$$

where the decryption error is negligible.

2. Verification correctness.

Verification correctness is satisfied using an AB-VCPRE scheme. We have the probability $\Pr\left[\text{Re}Enc - Ver(VK_{\alpha\to\beta}, CT_\alpha, CT_\beta) = 1\right] = 1$ if all converted ciphertexts CT_β are produced by the re-encryption keys $RK_{\alpha, f\to\beta}$ and Re$Enc(pp, RK_{\alpha, f\to\beta}, CT_\alpha)$.

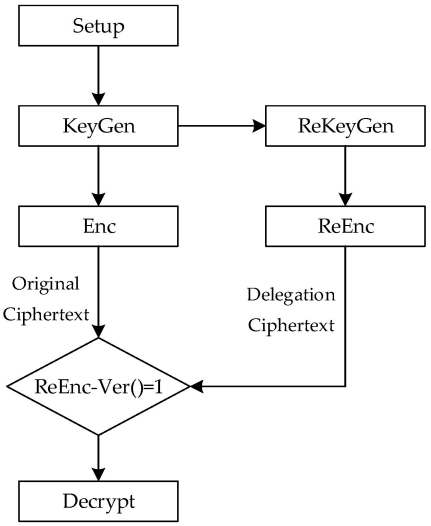

Figure 1. Flow chart of AB-VCPRE.

4.2. Security Model

Definition 6. *To demonstrate the CPA security of the AB-VCPRE scheme, the game between challenger $\mathcal{C}$ and adversary $\mathcal{A}$ is used.*

Init. Before seeing the public parameter pp, adversary $\mathcal{A}$ declares a vector of attributes x^*.

Setup. Initialize the public parameters pp in Challenger $\mathcal{C}$ and use the *KeyGen* algorithm to obtain (sk_θ, pk_θ), and transmit pp and pk_θ to $\mathcal{A}$.

Query phase 1. $\mathcal{A}$ chooses some queries as the following:

- *KeyGen query*$\mathcal{O}_{KeyGen}$: $\mathcal{A}$ performs a key query. $\mathcal{C}$ runs $KeyGen(pp, \beta)$ to produce the (pk_β, sk_β);
- Re*KeyGen query*$\mathcal{O}_{\mathrm{Re}KeyGen}$: $\mathcal{C}$ runs $\mathrm{Re}KeyGen\left(pp, sk_\alpha, pk_\beta, f\right)$ to provide $rk_{\alpha,f\to\beta}$ when $\mathcal{C}$ receives a re-encryption key query, where $f(x^*) = 0$ and $pk_\beta = KeyGen(pp, \beta)$. And $\mathcal{C}$ responds with verification key by running algorithm $HS.KeyGen(n, d^{hs}, N)$;
- Re*Enc query* $\mathcal{O}_{\mathrm{Re}Enc}$: $\mathcal{A}$ sends $(CT_\alpha,\ x,\ f)$ to $\mathcal{C}$ where $x \neq x^*$ and $f(x) = 0$, $\mathcal{C}$ computes a re-encryption key $rk_{\alpha,f\to\beta}$ as in $\mathcal{O}_{\mathrm{Re}KeyGen}$ and returns a re-encrypted ciphertext CT_β by running $\mathrm{Re}Enc\Big(pp, RK_{\alpha,f\to\beta}, CT_\alpha\Big)$.

Challenge phase. $\mathcal{A}$ chooses two messages of the same length μ_0^* and $\mu_1^*(\mu_0^* \neq \mu_1^*)$, $\mathcal{C}$ executives $CT^* \leftarrow Enc\left(pp, pk_\theta, x^*, \mu_b^*\right)$, where $b \in \{0,1\}$, and gives back the original ciphertext from CT^* to $\mathcal{A}$.

Query phase 2. Similar to phase 1, $\mathcal{A}$ keeps asking the query.

Guess. $b' \in \{0,1\}$ is guessed by $\mathcal{A}$, and if $b = b'$, the game winner is $\mathcal{A}$.

The benefits of $\mathcal{A}$ are described as $\Pr[b' = b] = 1/2 + negl(n)$.

5. Our Scheme

5.1. Our Scheme Composition

Using the LWE difficulty problem as a basis and the homomorphic signature algorithm, this paper proposes an AB-VCPRE scheme.

1. $Setup(n)$

Let security parameters $n \in Z$, where $m \geq \lceil 6n\log(q)\rceil$, $q/4 \geq B \cdot (m+1)^{O(d)}$.

① Central agency generates random security parameters prime q, an error sampling algorithm χ for B-bounded distributions, $B \geq \sqrt{\mathrm{n}} \cdot \omega(\log n)$. The boolean circuit's maximum depth is d, the number of attributes is ℓ, and the Gaussian parameter is σ, $\sigma = \omega\Big((\mathrm{m}+1)^{d+1}\Big) \cdot \omega\big(\sqrt{\log m}\big)$;

② Create the corresponding trapdoor matrix $T_{A_\alpha} \in \mathbb{Z}_q^{m\times m}$ and the matrix $A_\alpha \in \mathbb{Z}_q^{n\times m}$ by running algorithm $TrapGen(1^n, 1^m, q)$;

③ Select ℓ uniform matrices $B_1, \ldots, B_\ell \in \mathbb{Z}_q^{n\times m}$ with random.

④ Output public parameters $pp := \Big(\{B_i\}_{i\in[\ell],\chi}, \chi\Big)$.

2. $KeyGen(pp, \alpha)$

Randomly select a matrix $D_\alpha \in \mathbb{Z}_q^{n\times m}$, and run $R_\alpha \leftarrow Sample\mathrm{Pre}(A_\alpha, T_\alpha, D_\alpha, \sigma)$, such that $A_\alpha R_\alpha = -D_\alpha$.

Output $pk_\alpha = (A_\alpha, D_\alpha), sk_\alpha = (R_\alpha, T_\alpha)$.

3. $Enc(pp, pk_\alpha, \mu, x)$

① Given the plaintext $\mu \in \{0,1\}^m$, attribute vectors $x \in \{0,1\}^\ell$, where $x = \{x_i\}_{i\in[\ell]}$. Select random vectors $s \leftarrow \mathbb{Z}_q^n$, error vectors $e_1, e_2 \leftarrow \chi^m$;

② Compute $cc = (c_1, c_2)$:

$$c_1 = A_\alpha^T s + e_1, c_2 = D_\alpha^T s + e_2 + \lfloor q/2 \rfloor \mu.; \tag{7}$$

③ ca should be set to $\varnothing$ if x is null or none. Or else randomly choose ℓ uniform matrices $S_i \leftarrow \{-1,1\}^{m\times m}$ at random, calculate

$$ca = \left(\left\{c_i = (x_i G + B_i)^T s + S_i^T e_1\right\}_{i\in[\ell]}\right) \in \mathbb{Z}_q^{\ell m}. \tag{8}$$

Output ciphertext $CT_\alpha := (cc, ca)$;

4. $Dec(pp, sk_\alpha, CT_\alpha)$

Input $sk_\alpha = (R_\alpha, T_\alpha)$, $CT_\alpha = (cc, ca)$.

① Compute $\hat{\mu} = c_2 + R_\alpha^T c_1$. Set $\mu_i = 1$ for $i \in [m]$ if $|q/2 - \hat{\mu}_i| < q/4$, or else set $\mu_i = 0$.

Output $\mu \in \{0,1\}^m$;

5. Re$KeyGen(pp, sk_\alpha, pk_\beta, f)$

Input $pk_\beta = (A_\beta, D_\beta)$, $sk_\alpha = (T_\alpha, R_\alpha)$, $pp = \left(\{B_i\}_{i\in[\ell],\chi}, \chi\right)$, a policy $f \in \mathcal{F}_{\ell.d}$.

① Randomly selected matrices $E_1 \leftarrow \chi^{2km\times n}$, $E_2, E_3 \leftarrow \chi^{2km\times m}$, s is the Gaussian parameter, and $s = \omega((m+1)^{d+3/2})$.

② Let $B_f = Eval_{pk}(f, B_1, \ldots, B_\ell)$, $F = (A_\alpha | B_f) \in \mathbb{Z}^{n\times 2m}$. Running $T_{\alpha,f} \leftarrow SampleBasisLeft(A_\alpha, B_f, T_\alpha, s)$. Generate the basic $T_{\alpha,f}$ for F.

③ Execute algorithm $Sample$Pre$(F, T_{\alpha,f}, -D_\alpha, \sigma)$ to produce $R_{\alpha,f}$, in order to obtain $FR_{\alpha,f} = -D_\alpha$, of which $R_{\alpha,f} \in \mathbb{Z}^{2m\times m}$. Compute the re-encryption key:

$$Q = \begin{bmatrix} E_1 A_\beta + E_2 & E_1 D_\beta + E_3 + Power2_q(R_{\alpha,f}) \\ 0_{m\times m} & \mathrm{I}_{m\times m} \end{bmatrix} \in \mathbb{Z}_q^{(2km+m)\times 2m}; \quad (9)$$

④ Creating the verification key using algorithm $HS.KeyGen(n, d^{hs}, N)$ and signature private key $(hsvk, hssk)$, parse each line of Q as $w_i \in \mathbb{Z}_q^{2m} (1 \le i \le 2mk + m)$, then use the signature algorithm to sign w_i as $\sigma_i = HS.Sign(hssk, w_i)$;

⑤ To validate the signature, publish $hsvk$. Deliver Q and the associated signature $\left\{RK_{\alpha,f\to\beta} = Q, \sigma_i (1 \le i \le 2mk + m)\right\}$ across a secure channel to the proxy server;

6. Re$Enc(pp, RK_{\alpha,f\to\beta}, CT_\alpha)$

Input $pp = \left(\{B_i\}_{i\in[\ell],\chi}, \chi\right)$, $RK_{\alpha,f\to\beta} = Q$, $CT_\alpha = (cc, ca)$.

① Output $\perp$ if $f(x) \neq 0$ or $ca = \varnothing$, or else $c_3 = Eval_{ct}(f, \{(x_i, B_i, p_i)\}_{i\in[\ell]})$, $\widetilde{c}_{1,3} = ([c_1; c_3])$. The proxy performs the ciphertext conversion $(c_1'^T | c_2'^T) = \left[\widetilde{c}_{1,3}^T \middle| c_2^T\right] \cdot Q$;

② The valuation circuit is $g_{C_\alpha}(Q) = \left[\widetilde{c}_{1,3}^T \middle| c_2^T\right] \cdot Q$, and the evaluation algorithm from HS creates a signature $\sigma_{\alpha\to\beta} = HS.SignEval(g_{C_\alpha}, \sigma_i (1 \le i \le 2mk + m))$.

Output $CT_\beta = \left(cc' = (c'_1, c'_2), ca' = \varnothing, \sigma_{\alpha\to\beta}\right)$ as converted ciphertext;

7. Re$Enc - Ver(hsvk, CT_\alpha, CT_\beta)$

Input verification key $hsvk$, original ciphertext $CT_\alpha = (cc = (c_1, c_2), \sigma_{*\to\beta})$, converted ciphertext $CT_\beta = (cc' = (c'_1, c'_2), \sigma_{\alpha\to\beta})$.

Verification algorithm output $HS.Verify(hsvk, g_{C_\alpha}, cc', \sigma_{\alpha\to\beta})$.

Figure 2 depicts the new AB-VCPRE scheme's workflow. If Bob wants to share Alice's content stored on the cloud server, first KGC generates a public key and private key for Alice and Bob and sends the keys to them. Then, Alice generates the re-encryption key and original ciphertext, which are sent to the cloud server and executes the re-encryption algorithm. The cloud server delivers both the original and the re-encryption ciphertext to the authentication server after the re-encryption operation is finished. The authentication server verifies the algorithm for re-encryption. If the verification algorithm outputs 1, the authentication server sends Bob the ciphertext, Bob recovers the message by decrypting the ciphertext matching to it, otherwise output $\perp$.

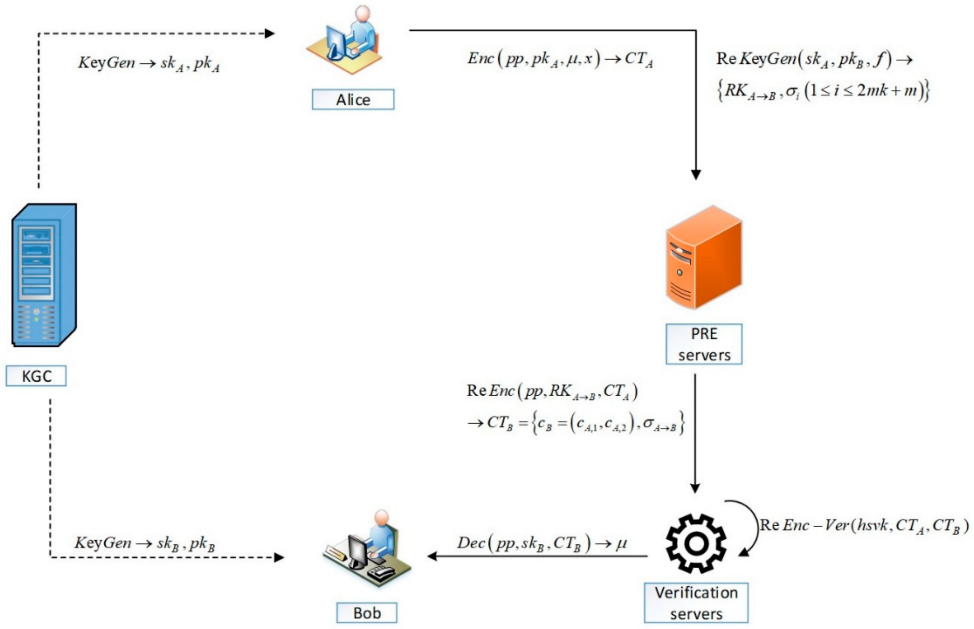

Figure 2. The workflow of AB-VCPRE.

5.2. Correctness and Parameters

5.2.1. The Correctness of the Original Ciphertext

With the private key R_α, the original ciphertext can be decrypted.

$$\begin{aligned} \hat{\mu} &= c_2 + R_\alpha^T c_1 \\ &= D_\alpha^T s + e_2 + \lfloor q/2 \rfloor \mu + R_\alpha^T \left(A_\alpha^T s + e_1 \right) \\ &= \underbrace{e_2 + e_1 R_\alpha}_{noise} + \lfloor q/2 \rfloor \mu \end{aligned} . \tag{10}$$

Only if the error $e_2 + e_1 R_\alpha$ does not exceed $q/4$ the decryption algorithm is able to correctly recover the plaintext μ. In fact, $\left|\left| e_2 + e_1 R_\alpha \right|\right| \leq \sqrt{m}B + m\sqrt{m}\sigma B \leq B \cdot (1 + \mathrm{m})^{O(d)} \leq q/4$.

5.2.2. Correctness of Conversion Ciphertext

After passing one conversion, the corresponding conversion cipher is decrypted as follows:

$$\begin{aligned} \left(c_1'^T \quad \middle| c_2'^T \right) &= \left[\tilde{c}_{1,3}^T | c_2^T \right] \cdot Q \\ &= \left[\tilde{c}_{1,3}^T | c_2^T \right] \cdot \begin{bmatrix} E_1 A_\beta + E_2 & E_1 D_\beta + E_3 + Power2_q\left(R_{\alpha,f} \right) \\ 0_{m \times m} & \mathrm{I}_{m \times m} \end{bmatrix} \\ &= \left[\tilde{c}_{1,3}^T \cdot \left(E_1 A_\beta + E_2 \right) | \tilde{c}_{1,3}^T \cdot \left(E_1 D_\beta + E_3 + Power2_q\left(R_{\alpha,f} \right) \right) + c_2^T \right] \\ &= \left[\tilde{c}_{1,3}^T \cdot \left(E_1 A_\beta + E_2 \right) | \tilde{c}_{1,3}^T \cdot \left(E_1 D_\beta + E_3 \right) + \tilde{c}_{1,3}^T \cdot Power2_q\left(R_{\alpha,f} \right) + D_\alpha s^T + e_2^T + \lfloor q/2 \rfloor \mu^T \right] \\ &= \left[\tilde{c}_{1,3}^T \cdot \left(E_1 A_\beta + E_2 \right) | \tilde{c}_{1,3}^T \cdot \left(E_1 D_\beta + E_3 \right) + \left[e_1^T | e_f^T \right] R_{\alpha,f} + e_2^T + \lfloor q/2 \rfloor \mu^T \right] \end{aligned} \tag{11}$$

where A_β and D_β are the user β's public keys, $\left|\left| E_1 \right|\right| \leq \sqrt{2k}mB$, $\left|\left| E_2 \right|\right| \leq \sqrt{2k}mB$, $\left|\left| E_3 \right|\right| \leq \sqrt{2k}mB$ with overwhelming probability. By the theorem we have:

$$\begin{aligned}\widetilde{c}_{1,3}^{T} \cdot Power2_q(R_{\alpha,f}) &= [c_1; c_3]^T \cdot R_{\alpha,f} \\ &= \left[c_1^T \middle| c_3^T\right] \cdot R_{\alpha,f} \\ &= \left[\left(s^T A + e_1^T\right) \middle| \left(s^T\left(f(x)G + B_f\right) + e_f^T\right)\right] \cdot R_{\alpha,f} \\ &= \left[\left(s^T A + e_1^T\right) \middle| \left(s^T B_f + e_f^T\right)\right] \cdot R_{\alpha,f} \\ &= \left[s^T\left[A_\alpha \middle| B_f\right] + \left[e_1^T \middle| e_f^T\right]\right] \cdot R_{\alpha,f} \\ &= -s^T D_\alpha + \left[e_1^T \middle| e_f^T\right] \cdot R_{\alpha,f}\end{aligned} \tag{12}$$

where $R_{\alpha,f} \leq \sqrt{2}m\sigma$, $\left|\left|e_f\right|\right| \leq B\sqrt{m}(m+1)^d$ with overwhelming probability.

The conversion ciphertext is decrypted by the private key R_β.

$$\begin{aligned}\left[c_1'^T \middle| c_2'^T\right] \cdot \begin{bmatrix} R_\beta \\ I \end{bmatrix} &= \widetilde{c}_{1,3}^{T}(E_1 A_\beta + E_2) \cdot R_\beta + \widetilde{c}_{1,3}^{T}(E_1 D_\beta + E_3) + \left[e_1^T \middle| e_f^T\right] R_{\alpha,f} + e_2^T + \lfloor q/2 \rfloor \mu^T \\ &= \underbrace{\widetilde{c}_{1,3}^{T} E_2 R_\beta + \widetilde{c}_{1,3}^{T} E_3 + \left[e_1^T \middle| e_f^T\right] R_{\alpha,f} + e_2^T}_{noise} + \lfloor q/2 \rfloor \mu^T\end{aligned} \tag{13}$$

where:

$$\left|\left|\widetilde{c}_{1,3}^{T} E_2 R_\beta + \widetilde{c}_{1,3}^{T} E_3 + \left[e_1^T \middle| e_f^T\right] R_{\alpha,f} + e_2^T\right|\right| \leq 2km^2\sqrt{m}\sigma B + 2km\sqrt{m}B + 2m\sqrt{m}(m+1)^d \sigma B + \sqrt{m}B \leq B(m+1)^{O(d)} \leq q/4 \tag{14}$$

with overwhelming probability. Therefore, the value of μ can be decrypted correctly, i.e., the transformed ciphertext can be decrypted correctly.

In fact, the algorithm can only obtain single-hop, because in ReEnc, we set $ca' = \varnothing$, which means that the re-encryption ciphertext cannot be encrypted again. This design is our first work and we will investigate this problem and extend it to multi-hop schemes in future work.

5.2.3. Correctness of Ciphertext Verification

In the HS scheme, the re-encryption verifiability is carried out using the algorithm $HS.Verify$. In $AB - VCPRE.\text{Re}Enc\left(pp, RK_{\alpha,f\to\beta}, CT_\alpha\right)$, input the ciphertext CT_α and the re-encryption key $RK_{\alpha,f\to\beta}$, using $g_{C_\alpha}(Q) = \left[Bits_q([c_1; c_3])^T \middle| c_2^T\right] \cdot Q$ as a valuation circuit, re-encryption key as circuit input, $(c_1'^T | c_2'^T) = \left[Bits_q([c_1; c_3])^T | c_2^T\right] \cdot Q$ can be seen as some computation at the message level and in $\sigma_{\alpha\to\beta} = HS.SignEval(g_{C_\alpha}, \sigma_i(1 \leq i \leq 2mk + m))$, with signature $\sigma_i(1 \leq i \leq 2mk + m)$ as input, and it can be interpreted as a computation of the signature level. If $\sigma_{\alpha\to\beta}$ is in fact the outcome of an honest computation based on $HS.SignEval(g_{C_\alpha}, \sigma_i(1 \leq i \leq 2mk + m)) = \sigma_{\alpha\to\beta}$, the concept of correctness for homomorphic signature schemes holds. Then $HS.Verify(hsvk, g_{C_\alpha}, cc', \sigma_{\alpha\to\beta})$ can pass the verification and the verification algorithm's accuracy is demonstrated.

5.3. Security

Theorem 1 (Security). *The scheme we construct is CPA security under $LWE_{n,q,\chi}$ assumption.*

Proof of Theorem 1. A game-based approach is used in this proof. A challenger $\mathcal{C}$ can be built to resolve the LWE presumption if it is possible for an adversary $\mathcal{A}$ to breach the CPA's security.

Game 0: In the original CPA attack paradigm described in Section 3, this is a true game between $\mathcal{A}$ and $\mathcal{C}$.

Game 1: Same as game 0, but with a change in the way the common matrix $\{B_i\}_{i\in[\ell]}$ is generated. On receipt of x^*, $\mathcal{C}$ generates ℓ uniformly random small parametric matrices $S_1^*, \ldots, S_\ell^* \in \{-1, 1\}^{m\times m}$, calculate $B_i = A^* S_i^* - x_i^* G$ where $i \in [\ell]$. □

Lemma 5. *Game 0 is statistically indistinguishable from game 1.*

Proof of Lemma 5. In game 0, $\{B_i\}_{i\in[\ell]}$ is a random uniform matrix on $\mathbb{Z}_q^{n\times m}$. In the challenge query, $\{S_i^*\}_{i\in[\ell]}$ is the construction of the generated challenge ciphertext c^* random matrix. However, in game 1, $e \in \chi^m$ serves as the error vector and S_i is used to generate B_i and c^*. By Lemma 2, the distribution $\left(A^*, \{A^*S_i^*\}_{i\in[\ell]}, e\right)$ and $\left(A^*, \{A_i^*\}_{i\in[\ell]}, e\right)$ are statistically equivalent for any $\{A_i^*\}_{i\in[\ell]} \in \mathbb{Z}_q^{n\times m}$. Hence, no statistically significant difference exists between the common matrix $\{B_i\}_{i\in[\ell]}$ in games 0 and 1. This shows that there is no statistically significant difference between games 0 and 1. □

Game 2: Challenger $\mathcal{C}$ randomly selects A_θ on $\mathbb{Z}_q^{n\times m}$ with no trapdoor and utilizes the *TrapGen* to produce B and its trapdoor T_B.

KeyGen query $\mathcal{O}_{KeyGen}$. $\mathcal{A}$ performs a key query. $\mathcal{C}$ run $KeyGen(pp, \beta)$ to produce the (pk_θ, sk_θ), output pk_β to $\mathcal{A}$.

ReKeyGen query $\mathcal{O}_{\mathrm{ReKeyGen}}$. When adversary $\mathcal{A}$ interrogates $\mathcal{O}_{\mathrm{ReKeyGen}}(pk_\alpha, pk_\beta, f)$ to make $f(x^*) \neq 0$, challenger $\mathcal{C}$ executes $Eval_{sim}$ of Lemma 4 to create a re-encryption key.

1. $pp = \left(\{B_i\}_{i\in[\ell]}, \chi\right)$, $pk_\beta = (A_\beta, D_\beta)$, policy $f \in \mathcal{F}_{\ell,d}$, set $B_f = Eval_{pk}(f, (B_1, \ldots, B_\ell))$, a policy $F = \left(A_\theta \middle| B_f\right) \in \mathbb{Z}^{n\times 2m}$;
2. Run $S_f^* \leftarrow Eval_{sim}\left(f, \{(S_i^*, x_i^*)\}_{i\in[\ell]}, A\right)$ to make $AS_f^* - f(x^*)G = B_f$. It follows from the definition of $Eval_{sim}$ that there is $\left|\left|S_f^*\right|\right|_2 < (1+m)^{d+1}$;
3. $\mathcal{C}$ executive $SampleBasisRight\left(A_\theta, G, S_f^*, T_G, s\right)$ to generate short basic $T_{\theta,f}$ of $\left(A_\theta \middle| B_f\right)$. Run $SamplePre\left(F, T_{\theta,f}, -D_\theta, \sigma\right)$ to produce $R_{\theta,f} \in \mathbb{Z}^{2m\times m}$, hence, an equals $FR_{\theta,f} = -D_\theta$;
4. When $f(x^*) \neq 0$, let $\overline{R}_{\alpha,f} = Power2_q\left(R_{\alpha,f}\right)$, matrix $E_1 \leftarrow \chi^{2km\times n}$, $E_2, E_3 \leftarrow \chi^{2km\times m}$, create the matrix

$$Q = \begin{bmatrix} E_1A_\beta + E_2 & E_1D_\beta + E_3 + Power2_q(\overline{R}_{\theta,f}) \\ 0_{m\times m} & \mathrm{I}_{m\times m} \end{bmatrix} \in \mathbb{Z}_q^{(2km+m)\times 2m}; \tag{15}$$

5. When $f(x^*) = 0$, let $\overline{R}_{\alpha,f} = Power2_q\left(R_{\alpha,f}\right)$, matrix $E_1 \leftarrow \chi^{2km\times n}$, $E_2, E_3 \leftarrow \chi^{2km\times m}$, select a random uniform distribution matrix $M \in \mathbb{Z}_q^{2km\times m}$, create the matrix

$$Q = \begin{bmatrix} E_1A_\beta + E_2 & M + \overline{R}_{\theta,f}) \\ 0_{m\times m} & \mathrm{I}_{m\times m} \end{bmatrix} \in \mathbb{Z}_q^{(2km+m)\times 2m}. \tag{16}$$

Then $\mathcal{A}$ send the challenger $\mathcal{C}$ some re-encryption verification questions, who will then carry out the operation honestly and report the results to the adversary $\mathcal{A}$.

ReEnc query $\mathcal{O}_{\mathrm{ReEnc}}$. $\mathcal{C}$ output $\mathrm{ReEnc}\left(pp, CT_\alpha, RK_{\theta,f\to\beta}\right)$.

Lemma 6. *Game 1 is computationally indistinguishable from game 2.*

Proof of Lemma 6. The technique employed to generate the re-encryption key differs between games 1 and 2. When $f(x^*) = 0$ hold, here is the re-encryption key:

$$rk_{\theta,f\to\beta} = \begin{cases} \begin{bmatrix} E_1A_\beta + E_2 & E_1D_\beta + E_3 + \overline{R}_{\theta,f} \\ 0_{m\times m} & \mathrm{I}_{m\times m} \end{bmatrix} & in\ Game\ 1 \\ \begin{bmatrix} E_1A_\beta + E_2 & M + \overline{R}_{\theta,f}) \\ 0_{m\times m} & \mathrm{I}_{m\times m} \end{bmatrix} & in\ Game\ 2 \end{cases} \tag{17}$$

Corollary 1. *By applying the standard mixing parameters, the ensuing distributions cannot be distinguished computationally. Otherwise, there is a useful algorithm for resolving the* $LWE_{n,q,\chi}$ *problem.*

1. $(D, DY + F)$ *and* (D, V), *where* $D \leftarrow \mathbb{Z}_q^{n\times m}$, $Y \leftarrow \chi^{\mathrm{m}\times\ell}$, $F \leftarrow \chi^{n\times\ell}$, $V \leftarrow \mathbb{Z}_q^{n\times\ell}$;
2. $(D, K, DY + F, KY + F')$ *and* $(D, K, DY + F, KY' + F')$, *where* $D, K \leftarrow \mathbb{Z}_q^{n\times m}$, $Y, Y', F, F' \leftarrow \chi^{n\times m}$;
3. $(D, \{DY_i + F_i\}_{i\in[t]})$ *and* $(D, \{V_i\}_{i\in[t]})$, *where* $D \leftarrow \mathbb{Z}_q^{n\times m}$, $Y_i \leftarrow \chi^{n\times m}$, $F_i \leftarrow \chi^{n\times\ell}$, $V_i \leftarrow \mathbb{Z}_q^{n\times\ell}$ *for* $i \in [t]$, $t = poly(n)$.

By Corollary 1, under the LWE assumption, it is evident that game 1 and game 2 are computationally indistinguishable.

Additionally, the private key creation mechanism is undetected from game 1 to game 2, and the produced private key continues to satisfy $A_\alpha R_\alpha = D_\alpha$, while the re-encryption key is selected from the uniform distribution, which is similar to the standard LWE distribution. Furthermore, because homomorphic signatures are non-negligible, the adversary in the CPA game cannot offer an invalid ciphertext to pass re-encryption verification, that is, re-encryption verification provides no auxiliary capacity to the adversary.

On the other side, to demonstrate it, if $\mathcal{A}$ succeeds in the re-encryption verifiability game, then by interacting with challenger $\mathcal{C}$, the simulator $\mathcal{S}$ can break the homomorphic signature's unforgeability.

The verification key *hsvk* is first acquired by the simulator $\mathcal{S}$ from $\mathcal{C}$. The re-encryption key $RK^*_{\theta,f\to\beta}$ is then chosen by adversary $\mathcal{A}$ as the one it wants to assault, and the simulator s is provided $RK^*_{\theta,f\to\beta}$ by $\mathcal{A}$. To create the signature, $\mathcal{S}$ asks the message $RK^*_{\theta,f\to\beta}$ for a homomorphic signature to obtain $\sigma_i (1 \le i \le 2mk + m)$ and then gives it back to $\mathcal{A}$. The challenger $\mathcal{C}$ then calculates $HS.Verify\left(hsvk, g_{C_\alpha}, cc^*, \sigma^*_{\theta\to\beta}\right)$ whenever $\mathcal{A}$ outputs a false re-encryption ciphertext $CT^*_\beta = \left(cc^* = (c_1^*, c_2^*), ca^* = \varnothing, \sigma^*_{\theta\to\beta}\right)$ after the simulator $\mathcal{S}$ has parsed it, where g_{C_α} is an evaluation circuit converted from the original ciphertext.

If $\mathcal{A}$ wins the verifiability of re-encryption, the forgery of $\mathcal{A}$'s signature $\sigma^*_{\theta\to\beta}$ can pass $HS.Verify$, which also counts as a valid homomorphic signature. Therefore, breaking the unforgeability of the homomorphic signature provides the same advantage as breaking the re-encryption verifiability of the AB-VCPRE scheme. When all of the aforementioned factors are considered, game 1 and game 2 are similar from the standpoint of the adversary. □

Game 3: Similar to game 2, except that the challenge cipher $CT^* = (c_1^*,\ c_2^*) \in \mathbb{Z}^{2m\times 1}$ given to the opponent is no longer honestly generated, but chosen evenly and randomly in $\mathbb{Z}^{2m\times 1}$. Due to the fact that the challenge cipher is a random factor in the cipher space, it is independent of μ_0^* and μ_1^*, so there is zero advantage to the $\mathcal{A}$ in this game.

Lemma 7. *Game 2 is statistically indistinguishable from game 3.*

Proof of Lemma 7. If $\mathcal{A}$ distinguishes game 2 from game 3 with a non-negligible advantage, then there is a simulator $\mathcal{S}$ that can use the information acquired by $\mathcal{A}$ to resolve the $LWE_{n,q,\chi}$ problem. □

LWE instance. The simulator $\mathcal{S}$ requests the LWE prophesy device to acquire an LWE instance $(Y, b) \in \mathbb{Z}_q^{n\times 2m} \times \mathbb{Z}_q^{2m}$, possibly (Y, b) is a truly random distribution or $b = Y^T s + e$ is a pseudo-random distribution of noise $e \in \chi^m$ from the LWE.

Public parameters. Let $[A_\theta | D_\theta] := Y$, sample a uniform matrix $D_\theta \leftarrow \mathbb{Z}_q^{n\times m}$ to generate a randomly identified public key $A_\theta \leftarrow \mathbb{Z}_q^{n\times m}$, select ℓ random matrices $\left(S_1^*, \ldots, S_\ell^*\right) \leftarrow \{-1, 1\}^{m\times m}$, and let $B_i = A_\theta S_i^* - x_i^* G$ for $i \in [\ell]$. Then the common matrix $pp = \left(\left\{B_i = A_\theta S_i^* - x_i^* G\right\}_{i\in[\ell],\ \chi}\right)$, public key $pk := (A_\theta, D_\theta)$.

Queries. As with game 2, $\mathcal{B}$ answers all of $\mathcal{A}$'s queries.

Challenge ciphertext. Generate challenge cipher via LWE instance

$$[c_1; c_2] := z; \tag{18}$$

$$\left[c_{11}^T \middle| \ldots \middle| c_{\ell\ell}^T\right] = c_1^T [S_1^* | \ldots | S_\ell^*]. \tag{19}$$

The answer to $\mathcal{A}$ is then returned. In this case, the distribution of the challenge cipher is the same as that of game 2.

$$\begin{aligned} z &= [c_1; c_2] \\ &= Y^T s + e \\ &= [A_\theta | D_\theta]^T s + [e_1; e_2] \end{aligned} \tag{20}$$

where $Y \leftarrow \mathbb{Z}_q^{n \times 2m}$, $s \leftarrow \mathbb{Z}_q^n$, $e \leftarrow \chi^{2m}$.

Challenge ciphertext:

$$c_1 = A_\theta^T s + e_1, c_2 = D_\theta^T s + e_2 + \lfloor q/2 \rfloor \mu; \tag{21}$$

$$ca = \left\{ c_i = (x_i^* G + B_i)^T s + (S_i^*)^T e_1 \right\}_{i \in [\ell]}. \tag{22}$$

Then through $B_i = A_\theta S_i^* - x_i^* G$, there is

$$\begin{aligned} \left[c_{11}^T | \ldots | c_{\ell\ell}^T\right] &= \left[s^T A_\theta S_1^* + e_1^T S_1^* | \ldots\ldots | s^T A_\theta S_\ell^* + e_1^T S_\ell^*\right] \\ &= \left(s^T A_\theta + e_1^T\right) \left[S_1^* | \ldots\ldots | S_\ell^*\right]. \end{aligned} \tag{23}$$

Statistically, the challenge ciphertext is indistinguishable in the alternative scenario if Y and z are chosen consistently, according to the leftover hash lemma [25].

Output. The simulator $\mathcal{S}$ outputs $\mathcal{A}$'s guess after $\mathcal{A}$ predicts whether it interacts with game 2 or game 3. $\mathcal{S}$ can solve the $LWE_{n,q,2m,\chi}$ problem with the same probability if $\mathcal{A}$ can distinguish between games 2 and 3. However, the $LWE_{n,q,2m,\chi}$ problem is mysterious, so game 3 cannot be won by $\mathcal{A}$.

The Proof of Theorem 1 is completed by considering game 0 to game 3.

Theorem 2 (Robustness). *The new AB-VCPRE scheme fulfills robustness if the homomorphic signature* Π_{HS} *satisfies unforgeability.*

Proof of Theorem 2. Using a randomly selected evaluation circuit, a dishonest proxy server is able to obtain an invalid re-encryption ciphertext share and corresponding signature. However, the original ciphertext should describe the right evaluation circuit. When the correct evaluation circuit diverges from the forgery, verification fails, allowing the proxy server to convert the data truthfully.

Homomorphic signatures can be used to demonstrate the robustness of the new scheme. If $\mathcal{A}$ can defeat the game outlined in Definition 6, then by collaborating with $\mathcal{C}$ in the homomorphic signature security model, it is able to build a simulator $\mathcal{S}$ that compromises the homomorphic signatures' unforgeability. Here is the procedure.

$\mathcal{A}$ picks the re-encryption key it wishes to attack once the simulator $\mathcal{S}$ receives the challenger $\mathcal{C}$'s verification key *hsvk*. When $\mathcal{A}$ sends simulator $\mathcal{S}$ a forged re-encryption ciphertext share $CT_\beta^* = \left(cc^* = (c_1^*, c_2^*), ca^* = \varnothing, \sigma_{\theta \to \beta}^*\right)$, $\mathcal{S}$ processes it to obtain $\left(hsvk, cc^* = (c_1^*, c_2^*), g_{C_\alpha}, \sigma_{\theta \to \beta}^*\right)$ and submits it to an oracle as a forged homomorphic signature.

If $\mathcal{A}$ succeeds in the robustness game, then $CT_\beta^* \neq \mathrm{Re}Enc\left(pp, RK_{\theta, f \to \beta}, CT_\theta\right)$, but $HS.Verify(hsvk, cc^*) = 1$, this also means that $HS.Verify\left(hsvk, g_{C_\alpha}, cc^*, \sigma_{\theta \to \beta}^*\right)$ was able to pass the verification, so the simulator $\mathcal{S}$ successfully forged an illegal signature, which will be submitted to oracle later. This indicates that the homomorphic signature algorithm's unforgeability has been compromised.

Thus, if the homomorphic signature algorithm Π_{HS} meets the requirement for unforgeability, the signature is considered unforgeable. The new AB-VCPRE is capable of achieving robustness. □

Theorem 3 (Weak collusion resistance). *The new AB-VCPRE scheme can realize weak collusion resistance, if the LWE problem is difficult.*

Proof of Theorem 3. Weak collusion resistance is that when an agent with a re-encryption key colludes with a trustee with a re-encryption key, the agent obtains only an approximate result, not an exact result.

The re-encryption key is $E_1A_\beta + E_2$ and $E_1D_\beta + E_3 + Power2_q(R_{\alpha,f})$, which can be further expressed as

$$\begin{bmatrix} A_\beta \\ D_\beta \end{bmatrix}, E_1 \begin{bmatrix} A_\beta \\ D_\beta \end{bmatrix} + \begin{bmatrix} E_2 \\ E_3 + Power2_q\left(R_{\alpha,f}\right) \end{bmatrix} \tag{24}$$

This is a standard LWE distribution that is not different from unified distribution, nor can anyone obtain any useful information about private keys. After collusion, Bob encrypted the above equation with his private key R_β and got $E_2R_\beta + E_3 + Power2_q\left(R_{\alpha,f}\right)$. As the noise generated during re-encryption is very low, the encryption message can be well restored by $E_2R_\beta + E_3 + Power2_q\left(R_{\alpha,f}\right)$. Therefore, in the case of collusion, the private key seems to have all been compromised. However, this is not the case. We can restore an equivalent private key, but this equivalent private key is different from the original private key. We provide the following two explanations. On the one hand, any data that can initially be decrypted by SK_α can be easily re-encrypted and read by an enemy who possesses both $RK_{\alpha,f\to\beta}$ and SK_β. On the other hand, they are unable to determine the delegator's precise private key SK_α from the equation above. Although Power2 is an easy-to-reverse feature, because it contains some noise from $E_2R_\beta + E_3$, you cannot obtain an exact private key from the first n-line of $E_2R_\beta + E_3 + Power2_q\left(R_{\alpha,f}\right)$. Therefore, the method proposed in this project has weak collusion resistance. □

6. Efficiency Analysis

Paper [15] proposed a CPRE algorithm based on DBDH, which supports fine-grained authorization and collision resistance security, however, it cannot achieve robustness. Paper [11] and paper [12] are PRE schemes with verification, both of which are robust and the method for achieving robustness is zero-knowledge proof with a decisional discrete logarithm tool, but are not as low complexity as the schemes in this paper. In addition, paper [12] is based on discrete logarithmic constructions and is not resistant to quantum attacks. Although paper [11] is a scheme using lattice construction, which seems to be resistant to quantum attacks, the robustness verification tool is a decisional discrete logarithm, so in general the scheme is not resistant to quantum attacks. Table 1 demonstrates that the approach presented in this paper is not only robust to proxy re-encryption but also simple to implement and resistant to quantum attacks.

Table 1. Comparison of related work.

	Construction Tool	Resisting Quantum Attack	Robustness	Method for Robustness	Tool for Robustness
Scheme [15]	DBDH	No	No	None	None
Scheme [12]	Discrete logarithm	No	Yes	zero-knowledge proof	Decisional discrete logarithm
Scheme [11]	Lattice	No	Yes	zero-knowledge proof	Decisional discrete logarithm
Our scheme	Lattice	Yes	Yes	Homomorphic signature	Lattice

In Table 2, the efficiency of the scheme is analyzed through plaintext space, size of ciphertext, size of re-encryption key, encryption complexity, re-encryption complexity, and robustness verification complexity. $|\mathbb{Z}_q|$ represents an integer on modulo q. T_p, T_e, T_s, T_v, and T_m denote the computation of pairing, modular exponentiation, signature, ciphertext verification, and multiplication operation, respectively. T_h, T_{GVP}, respectively, represent the time spent for the hash function and the GVP algorithm. Table 2 demonstrates that the computational complexity of the literature [15] is worse than that of the proposed scheme, and is not robust. In terms of robustness verification complexity, when a boolean circuit evaluates the original signature, homomorphic signature computation is a boolean operation that is more straightforward and effective. Here, we choose the linear homomorphic signature scheme based on the difficult problem of SIS on the lattice proposed in paper [26] for comparison. Compared with the scheme [12], the proposed scheme has better re-encryption complexity, encryption complexity, and robustness verification complexity. Compared with the scheme [11], the proposed scheme in this paper only needs to pay some extra cost to encrypt the message vector, and the robustness verification complexity is lower.

Table 2. Computational and communication complexity comparison.

	Message	**Size of Ciphertext**	**Size of Re-Encryption Key**	**Encryption Complexity**	**Re-Encryption Complexity**	**Verification Complexity**
Scheme [15]	$\{0,1\}$	$8\|\mathbb{Z}_q\|$	$8\|\mathbb{Z}_q\|$	$T_p + 8T_e + T_s$	$2T_p + T_e + T_v$	None
Scheme [12]	$\{0,1\}^m$	$4\|\mathbb{Z}_q\|$	$6\|\mathbb{Z}_q\|$	$3T_e + T_m$	$3T_e + T_m$	$2T_e + T_h$
Scheme [11]	$\{0,1\}$	$(n+1)\|\mathbb{Z}_q\|$	$(nm+1)(n+1)\|\mathbb{Z}_q\|$	$2T_m$	$2T_m$	$(nm+1)(\mathrm{n}+1)T_e$
Our scheme	$\{0,1\}^m$	$(\ell+2)m\|\mathbb{Z}_q\|$	$(4k+2)m^2\|\mathbb{Z}_q\|$	$5T_m$	$3T_m + T_s$	$T_h + T_{GVP}$

7. Conclusions

By using homomorphic signatures, this paper proposes an AB-VCPRE scheme, which solves the problem of being unable to detect illegal proxy behavior in traditional PRE schemes. The scheme is robust enough to allow proxy servers that have sent invalid transformed ciphertext shares to be detected. In terms of security, the scheme is CPA security based on a LWE problem and is resistant to quantum attacks. In terms of efficiency, the scheme has advantages in re-encryption and robustness verification computational efficiency. In addition, there is some room for improvement in the performance of our solutions, and constructing a multi-hopping PRE scheme will be the focus of our next work.

Author Contributions: Conceptualization, Y.T., M.J. and H.M.; methodology, M.J. and H.M.; validation, M.J., Y.T. and H.M.; formal analysis, M.J. and L.Y.; writing—original draft preparation, M.J.; writing—review and editing, H.M., C.Z. and L.Y.; supervision, H.M. and C.Z.; funding acquisition, Y.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research is partially supported by the Henan Key Laboratory of Network Cryptography Technology (LNCT2022-A11) and the Shaanxi Key Laboratory of Information Communication Network and Security (ICNS202006).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Blaze, M.; Bleumer, G.; Strauss, M. Divertible protocols and atomic proxy cryptography. In Proceedings of the Advances in Cryptology—EUROCRYPT'98: International Conference on the Theory and Application of Cryptographic Techniques, Espoo, Finland, 31 May–4 June 1998; pp. 127–144. [CrossRef]
2. Green, M.; Ateniese, G. Identity-based proxy re-encryption. In Proceedings of the Applied Cryptography and Network Security: 5th International Conference, ACNS 2007, Zhuhai, China, 5–8 June 2007; pp. 288–306. [CrossRef]
3. Weng, J.; Deng, R.H.; Ding, X.; Chu, C.-K.; Lai, J. Conditional proxy re-encryption secure against chosen-ciphertext attack. In Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, Sydney, Australia, 10–12 March 2009; pp. 322–332. [CrossRef]
4. Sahai, A.; Waters, B. Fuzzy identity-based encryption. In Proceedings of the Advances in Cryptology–EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 24–26 May 2005; pp. 457–473. [CrossRef]
5. Zamite, J.; Domingos, D.; Silva, M.J.; Santos, C. Group-based discretionary access control in health related repositories. *J. Inf. Technol. Res. JITR* **2014**, *7*, 78–94. [CrossRef]
6. Zhao, J.; Feng, D.; Zhang, Z. Attribute-based conditional proxy re-encryption with chosen-ciphertext security. In Proceedings of the 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, Miami, FL, USA, 6–10 December 2010; pp. 1–6. [CrossRef]
7. Liang, X.; Cao, Z.; Lin, H.; Shao, J. Attribute based proxy re-encryption with delegating capabilities. In Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, Sydney, Australia, 10–12 March 2009; pp. 276–286. [CrossRef]
8. Yang, Y.; Lu, H.; Weng, J.; Zhang, Y.; Sakurai, K. Fine-grained conditional proxy re-encryption and application. In Proceedings of the Provable Security: 8th International Conference, ProvSec 2014, Hong Kong, China, 9–10 October 2014; pp. 206–222. [CrossRef]
9. Mao, X.; Li, X.; Wu, X.; Wang, C.; Lai, J. Anonymous attribute-based conditional proxy re-encryption. In Proceedings of the Network and System Security: 12th International Conference, NSS 2018, Hong Kong, China, 27–29 August 2018; pp. 95–110. [CrossRef]
10. Ge, C.; Susilo, W.; Wang, J.; Huang, Z.; Fang, L.; Ren, Y. A key-policy attribute-based proxy re-encryption without random oracles. *Comput. J.* **2016**, *59*, 970–982. [CrossRef]
11. Li, J.; Ma, C.; Zhao, Q. Resplittable threshold multi-broker proxy re-encryption scheme from lattices. *J. Commun.* **2017**, *38*, 157–164.
12. Nunez, D. *Umbral: A Threshold Proxy Re-Encryption Scheme*; NuCypher Inc. and NICS Lab, University of Malaga: Málaga, Spain, 2018.
13. Luo, F.; Al-Kuwari, S.; Wang, F.; Chen, K. Attribute-based proxy re-encryption from standard lattices. *Theor. Comput. Sci.* **2021**, *865*, 52–62. [CrossRef]
14. Huang, Q.; Yang, Y.; Fu, J. PRECISE: Identity-based private data sharing with conditional proxy re-encryption in online social networks. *Future Gener. Comput. Syst.* **2018**, *86*, 1523–1533. [CrossRef]
15. Yao, S.; Dayot, R.V.J.; Kim, H.-J.; Ra, I.-H. A novel revocable and identity-based conditional proxy re-encryption scheme with ciphertext evolution for secure cloud data sharing. *IEEE Access* **2021**, *9*, 42801–42816. [CrossRef]
16. Ajtai, M. Generating hard instances of lattice problems. In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, Philadelphia, PA, USA, 22–24 May 1996; pp. 99–108. [CrossRef]
17. Agrawal, S.; Boneh, D.; Boyen, X. Efficient lattice (h) ibe in the standard model. In Proceedings of the Eurocrypt 2010, Berlin, Heidelberg, 30 May–3 June 2010; pp. 553–572.
18. Regev, O. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM JACM* **2009**, *56*, 1–40. [CrossRef]
19. Aono, Y.; Boyen, X.; Phong, L.T.; Wang, L. Key-private proxy re-encryption under LWE. In Proceedings of the Progress in Cryptology–INDOCRYPT 2013: 14th International Conference on Cryptology in India, Mumbai, India, 7–10 December 2013; pp. 1–18. [CrossRef]
20. Boneh, D.; Gentry, C.; Gorbunov, S.; Halevi, S.; Nikolaenko, V.; Segev, G.; Vaikuntanathan, V.; Vinayagamurthy, D. Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits. In Proceedings of the Advances in Cryptology–EUROCRYPT 2014: 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, 11–15 May 2014; pp. 533–556. [CrossRef]
21. Gorbunov, S.; Vaikuntanathan, V.; Wee, H. Predicate encryption for circuits from LWE. In Proceedings of the Advances in Cryptology—CRYPTO 2015: 35th Annual Cryptology Conference, Santa Barbara, CA, USA, 16–20 August 2015; pp. 503–523. [CrossRef]
22. Brakerski, Z.; Vaikuntanathan, V. Constrained Key-Homomorphic PRFs from Standard Lattice Assumptions: Or: How to Secretly Embed a Circuit in Your PRF. In Proceedings of the Theory of Cryptography: 12th Theory of Cryptography Conference, TCC 2015, Warsaw, Poland, 23–25 March 2015; pp. 1–30. [CrossRef]
23. Kim, S.; Wu, D.J. Watermarking PRFs from lattices: Stronger security via extractable PRFs. In Proceedings of the Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2019; pp. 335–366. [CrossRef]

24. Liang, X.; Weng, J.; Yang, A.; Yao, L.; Jiang, Z.; Wu, Z. Attribute-based conditional proxy re-encryption in the standard model under LWE. In Proceedings of the Computer Security–ESORICS 2021: 26th European Symposium on Research in Computer Security, Darmstadt, Germany, 4–8 October 2021; pp. 147–168. [CrossRef]
25. Håstad, J.; Impagliazzo, R.; Levin, L.A.; Luby, M. A pseudorandom generator from any one-way function. *SIAM J. Comput.* **1999**, *28*, 1364–1396. [CrossRef]
26. Deng, Y. A Linearly Homomorphic Signature Scheme on Lattice. *Henan Sci.* **2015**, *33*, 1346–1351.