Hierarchical and Efficient Identity-based Encryption Against Side Channel Attacks

Qihong Yu[1], Jian Shen[2], Jiguo Li[3], Sai Ji[4]
College of Information Engineering, Suqian University, Suqian, China[1]
School of Computer Science and Technology, Zhejiang SCI-TECH University, Hangzhou, China[2]
College of Computer and Cyber Security, Fujian Normal University, Fuzhou, China[3]
College of Information Engineering, Taizhou University, Taizhou, China[4]

***Abstract*—Hierarchical and identity-based encryption (HIBE) is very valuable and widely used in many occasions. In the Internet of Things based on cloud services, efficient HIBE is likely to be applied to cloud service scenarios for the limited computing ability of some terminal devices. What's more, because of the insecurity of cryptographic systems caused by side channel attacks, the design of leakage resilient cryptographic scheme has attracted more and more cryptography researchers' attention. In this study, an efficient leakage resilient HIBE is constructed. (1) In essence, this given scheme contains a hierarchical ID-based key encapsulation system. By using the extractor to act on the encapsulated symmetric key, this proposed scheme may resist the disclosure for the symmetric key due to side channel attacks. The relative leakage ratio of the encapsulated key is close to 1. (2) We also construct a hierarchical identity-based hash proof system that provides the security of our scheme. The proposed scheme can not only resist side channel attacks, but also has short public key parameters and computational efficiency, which is very suitable for applications in the Internet of Things environment. (3) There is no limit to the hierarchy depth of the system, and only the maximum hierarchy length is required to be given when the system is initialized.**

Keywords*—*Identity-based encryption; side channel attack; hash proof system; composite order group

I. INTRODUCTION

The hierarchical identity based encryption (HIBE) scheme has many practical applications. Pavithran et al. [1] constructed a blockchain structure with privacy protection suitable for the Internet of Things (IoT) through HIBE. Their scheme is very suitable for some terminal devices with limited computing resources. The practicability of the scheme is demonstrated through the traffic radar speed measurement system. Fan et al. [2] constructed an efficient data protection scheme of Message Queuing Telemetry Transport (MQTT) through HIBE. MQTT is widely used for the transmission and communication.

The researches [3] and [4] all gave HIBE schemes in the random oracle model. The given scheme in the study [3] does not affect the security of the system due to the hierarchy depth. Based on Bilinear Diffie Hellman (BDH) assumption, HIBE against collusion attack is given in the study [3].

The research [4] introduced the concept of HIBE and security. A concrete two-layer HIBE scheme is given. The upper layer is completely collusion-resistant, while the lower layer is only partially collusion-resistant. Based on BDH assumption, the security of the scheme is proved in the random oracle model.

The study [5] proposed HIBE which is not affected by the depth of hierarchy, and the key length and decryption cost are fixed. The ciphertext is fixed to three elements, and decryption requires only two bilinear map operations.

The research [6] gave HIBE that is not affected by the depth of hierarchy, and the ciphertext of the proposed scheme has a shorter length. Through the dual system encryption technology, they obtained the full security of the scheme based on the three static assumptions of the composite order group.

The dual system encryption technology is also considered in the research [7], but they constructed secure schemes in prime order groups. In particular, they presented new randomization and parameter-hiding techniques in prime-order groups.

Considering the efficiency of HIBE, the authors in [8] presented an efficient HIBE scheme. This study fully considered the effect of the system parameters, and improved the existing scheme by appropriately reducing unnecessary parameters.

Although there are some leakage resilient (LR) encryption schemes, there are few efficient LR encryption schemes. There are usually two types of means to solve efficiency problems. First, by properly optimizing parameter settings and removing unnecessary parameters, one may obtain an efficient scheme. Second, the scheme in the composite order group is transformed into the scheme in the prime order group. In this research, we will reduce the parameters appropriately by removing unnecessary parameters, so as to achieve the goal of high efficiency. This research constructs an efficient hierarchical identity based LR encryption scheme.

In this research, an efficient leakage resilient encryption scheme is explored. Through the use of extractor technology we obtain leakage resilient encryption scheme. Through the appropriate reduction of parameters we improve the efficiency of the system. Through the hash proof system we prove the security of the given system. This research provides an efficient leakage-resilient hierarchical identity-based encryption scheme that can resist almost all leakage of the encapsulated symmetric key. The relative leakage ratio of the encapsulated key is close to 1.

Other sections are arranged as follows. Section II gives the related works and our research motivation. Section III gives some necessary preparatory knowledge. Section IV gives the concrete scheme. Safety proof and leakage performance analysis are given in Section V. Section VI gives the performance comparison. The conclusion is given in Section VII.

II. Related Works

In the research [9], a new HIBE with the maximum hierarchy depth was proposed. When the system is initialized, the maximum hierarchy depth should be given. Considering the absolute trust of the root PKG and the incomplete trust of the sub PKG, it is impossible to delegate a private key for the next layer without the keys of other layers. In this way, the burden of key escrow is reduced.

Jiang et al. [10] presented a secure HIBE against chosen plaintext attacks (CPA). Using lattice theory, its CPA security is proved through learning with errors (LWE) theory. Making an additional point, an efficient HIBE is also proposed against adaptive chosen-ciphertext attacks (CCA). This scheme's security is provided through the shortcut vector problem (SVP) difficult assumption under random oracle model.

Emura et al. [11] has built an efficient HIBE through key isolation technology. They proposed a scheme called key-insulated HIBE (HKIBE). First, the pairing based HKIBE was constructed through the k-linear assumption under the standard model. Furthermore, they also gave a method to construct efficient HKIBE from general HIBE.

The study [12] gave a revocable identity-based (RIB) and authenticated key exchange (AKE). The scheme has these functions of decentralization and private key revocation. In addition, the general method of constructing hierarchical RIB-AKE from a hierarchical RIB key encapsulation mechanism is also given.

The authors [13] provided a functional encryption based on inner product under public key cryptosystem. When decryption is in progress, the decryptor's identity can be specified and this receiver's identity may be hierarchical. They also gave an experimental result to explain that their presented scheme has certain application value.

Langrehr and Pan [14] presented two adaptive and tight secure HIBE schemes. It is mainly constructed through Matrix Diffie-Hellman assumptions.

In order to resist quantum attacks, this study [15] constructed three hierarchical identity-based (HIB) schemes in the networks which can tolerate time delays. Through the lattice based LWE hypothesis, this study [15] proposed an HIB key agreement scheme, an HIB key update scheme and a non-interactive HIB key agreement scheme.

To avoid key exposure, this research [16] put forward the key isolated encryption technology. Shikata et al. [16] gave a hierarchical key insulated encryption scheme in the standard model.

The study [17] constructed the unbounded HIBE through double system groups and gave an example. This proposed scheme has shorter ciphertext and private key and has higher computational efficiency.

Zhang et al. [18] constructed anonymous HIBE in prime order groups. Its main advantage is that the private key and ciphertext are fixed in size.

The research [19] gave a CPA secure HIB broadcast encryption. This given scheme is based on prime order group which has high efficiency of computing. Then, the CPA secure scheme was converted to CCA secure scheme by one-time signature.

Some schemes have explored efficiency, such as the schemes [8, 11]. However, these schemes do not take into account the impact of side channel attacks, which may lead to the insecurity of the cryptographic systems.

A. Side Channel Attacks

In recent years, many side channel attacks have been discovered. The authors [20] made a study on the power analysis of pairing based cryptography implementation. The specific attack towards pairing cryptography scheme was given. Aiming at the typical lightweight encryption scheme LBlock, Weng et al. [21] presented an improved key differential analysis attack. The authors in [22] identified the keys by sound characteristics, and applied this attack to PIN pads. Chen et al. [23] exploited an attack in which an attacker may gain system's secret information from observing this timing and other characteristics of the cryptographic system.

Many researchers engage in leakage resilient (LR) cryptography research, and have constructed some encryption schemes with leakage resilience, such as LR public key encryption schemes [24, 25], LR identity-based encryption schemes [26, 27, 28, 29], LR attribute-based encryption schemes [30, 31, 32], LR certificate based encryption scheme [33, 34, 35], and leakage resilient certificateless encryption scheme [36, 37].

B. Our Motivations and Contributions

Inspired by the researches [6, 8], this study explores efficient encryption scheme in leakage resilient cryptography. An efficient HIBE with leakage resilience (LR-HIBE) is constructed.

First, the presented scheme has the function of resisting private key disclosure. By using the extractor, the given scheme may resist the leakage for the encapsulated symmetric key. It can resist the leakage of almost the entire encapsulated symmetric key.

Secondly, the presented scheme improves the overall performance of the system by reasonably reducing the parameters. Our scheme has less public key parameters. In addition, it greatly improves the efficiency of private key generation, private key delegation and encryption.

Furthermore, our scheme has good practicability and can greatly share the burden for the root private key generation center. The hierarchical function of the scheme enables the system to delegate private keys layer by layer. For example, we use Fig. 1 to show the information management system about Suqian University. Suqian University is the root. Those

colleges are the secondary nodes. These departments are the tertiary node, and the counselor or teacher is the leaf node. Let U represent the university. Let C represent the college. Let D represent the department. Let T represent the teacher. A member with the identity (Suqian University: School of Information Engineering) can delegate a private key to a member whose identity is (Suqian University: School of Information Engineering: Department of Software Engineering). However, he cannot delegate the private key to a member of (School: School of Management: Department of Accounting).

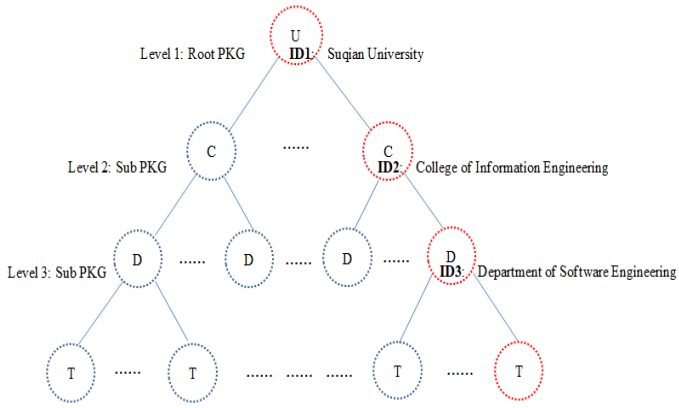

Fig. 1. The hierarchy of the information management system of Suqian University.

III. PRELIMINARIES

A. Bilinear Groups with Composite Order

The research [38] gave the definitions about bilinear groups with composite order (BG-CO). Let Ψ to denote a BG-CO generation algorithm, which inputs the safety parameter λ, and outputs a BG-CO $\Omega=\{N=v_1v_2v_3,G_1,G_2,e\}$, where $v_1,v_2,$ and v_3 are three different primes ($Log(v_1)=Log(v_2)=Log(v_3)$), G_1 is cyclic group with order N and G_2 is cyclic groups with order N. e is a bilinear mapping which satisfies the following two conditions.

1) Bilinearity.

$$\forall g_1,h_1\in G_1,a,b\in Z_N,e(g_1^a,h_1^b)=e(g_1,h_1)^{ab}$$

2) Non-degenerability. $\exists g_1\in G_1$ such that $e(g_1,g_1)\notin 1_{G_2}$.

Furthermore, it is required that the operations in groups G_1 and G_2 are computable in terms of the polynomial time about the security parameter λ. We use G_{v_1}, G_{v_2} and G_{v_3} to denote these subgroups in the group G_1 whose order is v_1, v_2 and v_3 respectively. In particular, when $d_i\in G_{v_i}$ and $d_j\in G_{v_j}$ ($i\neq j$), $e(d_i,d_j)$ is the identity for G_2. For example, supposing that $d_1\in G_{v_1}$, $d_2\in G_{v_2}$ and p is a generator for G_1, then $p^{v_1v_2}$ derives G_{v_3}, $p^{v_1v_3}$ derives G_{v_2}, $p^{v_2v_3}$ derives G_{v_1}. In this way, we can find α_1,α_2 such that $d_1=(p^{v_2v_3})^{\alpha_1}$ and $d_2=(p^{v_1v_3})^{\alpha_2}$. So, $e(d_1,d_2)=e(p^{v_2v_3\alpha_1},p^{v_1v_3\alpha 2})=e(p^{\alpha_1},p^{v_3\alpha_2})^{v_1v_2v_3}=1$. The G_{v_1}, G_{v_2} and G_{v_3} are orthogonal.

Three complexity assumptions are given here, which is going to be employed in the security proof.

We let $G_{v_1v_2}$ to express a subgroup with order v_1v_2. Other uses are similar.

Hypothesis 1. Given a composite order bilinear group generation algorithm Ψ and the distribution as follows.

$$\Omega=(N=v_1v_2v_3,G_1,G_2,e)\xleftarrow{R}\Psi,$$

$$g_1\xleftarrow{R}G_{v_1},X_3\xleftarrow{R}G_{v_3},$$

$$W=(\Omega,g_1,X_3),$$

$$T_1\xleftarrow{R}G_{v_1v_2},T_2\xleftarrow{R}G_{v_1}.$$

This advantage that one algorithm A breaks hypothesis 1 is defined as $Adv1_{\Psi,A}(\lambda):=|\Pr[A(W,T_1)=1]-\Pr[A(W,T_2)=1]|$.

According to the study [6], it is said that the algorithm Ψ satisfies hypothesis 1, if the advantage $Adv1_{\Psi,A}(\lambda)$ obtained by any probability polynomial adversary is negligible.

Hypothesis 2. Given a composite order bilinear group generation algorithm Ψ and the distribution as follows.

$$\Omega=(N=v_1v_2v_3,G_1,G_2,e)\xleftarrow{R}\Psi,$$

$$g_1,X_1\xleftarrow{R}G_{v_1},X_2,Y_2\xleftarrow{R}G_{v_2},X_3,Y_3\xleftarrow{R}G_{v_3},$$

$$W=(\Omega,g_1,X_1X_2,X_3,Y_2Y_3),$$

$$T_1\xleftarrow{R}G_1,T_2\xleftarrow{R}G_{v_1v_3}.$$

This advantage that one algorithm A breaks hypothesis 2 is defined as $Adv2_{\Psi,A}(\lambda):=|\Pr[A(W,T_1)=1]-\Pr[A(W,T_2)=1]|$.

According to the research [6], it is said that the algorithm Ψ satisfies hypothesis 2, if the advantage $Adv2_{\Psi,A}(\lambda)$ obtained by any probability polynomial adversary is negligible.

Hypothesis 3. Given a composite order bilinear group generation algorithm Ψ and the distribution as follows.

$$\Omega = (N = v_1 v_2 v_3, G_1, G_2, e) \xleftarrow{R} \Psi, \alpha, s \xleftarrow{R} Z_N,$$

$$g_1 \xleftarrow{R} G_{v_1}, X_2, Y_2, Z_2 \xleftarrow{R} G_{v_2}, X_3 \xleftarrow{R} G_{v_3},$$

$$W = (\Omega, g_1, g_1^{\alpha} X_2, X_3, g_1^{s} Y_2, Z_2),$$

$$T_1 \xleftarrow{R} e(g_1, g_1)^{\alpha s}, T_2 \xleftarrow{R} G_2 \text{。}$$

This advantage that one algorithm A breaks hypothesis 3 is defined as $Adv3_{\Psi,A}(\lambda) := |\Pr[A(W, T_1) = 1] - \Pr[A(W, T_2) = 1]|$.

According to the research [6], it is said that the algorithm Ψ satisfies hypothesis 3, if the advantage $Adv3_{\Psi,A}(\lambda)$ obtained by any probability polynomial adversary is negligible.

B. Binary Extractor

This statistical distance about two random variables P and Q is defined as: $STDS = \frac{1}{2}\sum_{\theta \in \Xi} |\Pr(P = \theta) - \Pr(Q = \theta)|$. This minimum entropy for a random variable P is defined as: $H_{\infty}(P) = -Log(\max_p \Pr(P = p))$.

The extractor [39]. We call a function $\text{Ext}: \{0,1\}^n \times \{0,1\}^r \to \{0,1\}^m$ as (k, ε) strong extractor as long as it meets the conditions. Suppose that U is the uniform distribution over $\{0,1\}^m$ and V is the uniform distribution over $\{0,1\}^r$. If $A \in \{0,1\}^n$ and $H_{\infty}(A) > k$, we can get that $STDS((Ext(A,V),V),(U,V)) \le \varepsilon$, where ε is a negligible value.

Conclusion 1 [40]. If P, Q and R are three random variables, and Q contains 2^{ξ} value where ξ is an integer which is used to express the upper bound of leakage, we get $\tilde{H}_{\infty}(P \mid (Q, R)) \ge \tilde{H}_{\infty}(P \mid R) - \xi$.

C. Hierarchical Identity-Based Hash Proof System

Inspired by the literature [40, 41, 42], we constructed a hierarchical identity-based hash proof system (HIB-HPS). The HIB-HPS includes the following algorithms: Setup, KeyG, Delegate, Encap, Encap*, and Decap.

Setup. This algorithm inputs a security parameter λ. It generates the public key parameter PK and the master private key MK. $Setup(\lambda) \to PK, MK$.

KeyG. This algorithm inputs MK and an identity vector $\vec{I}$. It gives the private key $SK_{\vec{I}}$. $KenG(MK, \vec{I}) \to SK_{\vec{I}}$.

Delegate. This algorithm takes an identity vector $\vec{I}$ with depth i and an identity ID_{i+1} as the input. It produces the private key $SK_{\vec{I}:ID_{i+1}}$ for this identity vector $\vec{I}:ID_{i+1}$ with depth $i+1$. $Delegate(PK, SK_{\vec{I}}, ID_{i+1}) \to SK_{\vec{I}:ID_{i+1}}$.

Encap. This algorithm inputs PK and $\vec{I}$. It generates (C, k). C expresses a correct ciphertext. k expresses an encapsulated key. $Encap(PK, \vec{I}) \to (C, k)$.

Encap*. This algorithm inputs PK and $\vec{I}$. It obtains an invalid ciphertext C. This algorithm is only used for the security proof. $Encap*(PK, \vec{I}) \to C$.

Decap. The algorithm inputs PK, C and a private key $SK_{\vec{I}}$. It produces an encapsulated key k. $Decap(PK, SK_{\vec{I}}, C) \to k$.

HIB-HPS has the three characteristics as follows.

1) Correctness

$$\Pr[k \ne k' \,|\, Encap(PK, \vec{I}) \to (C, k), Decap(PK, SK_{\vec{I}}, C) \to k'] < \varepsilon,$$

which means that the decapsulation algorithm are almost always right to obtain the encapsulation key. That is, if the encapsulation algorithm is used to obtain ciphertext C and the encapsulated key k, then the probability of the encapsulated key k obtained by the de encapsulation algorithm is $1\text{-}\varepsilon$ (ε is a negligible value).

2) Indistinguishability between the valid and invalid ciphertext.

Given a private key $SK_{\vec{I}}$, the ciphertext gained by the **Encap** algorithm is indistinguishable from the ciphertext generated by an invalid **Encap*** algorithm.

The indistinguishability is reflected by the next game which is played by an attacker A and a challenger C.

$\text{Game}_{\text{Real}}$

Initialize. C revokes the algorithm **Setup** to gain the public parameter PK. Let S denote the private key created by the challenger but not given to the attacker. The S is null at the beginning, i.e. $S = \phi$.

Phase 1. A carries on the private key creation inquiry ($-Create$), private key delegation inquiry ($-Delegate$), and private key inquiry ($-SK$).

$-Create$. A gives one identity vector $\vec{I}$. C calls the **KeyG** algorithm to obtain a private key and adds it in S. C only sends A a reference about the private key, not this private key itself.

$-Delegate$. A gives a private key $SK_{\vec{I}}$ in S and an identity ID. C connects ID and $\vec{I}$ to obtain $\vec{I}:ID$. Then, C generates a corresponding private key by calling the private key delegation algorithm. C only sends A a reference about the private key, not this private key itself.

$-SK$. A selects a specific element in S. C sends the private key to A. Then, C deletes it out of S. As for the private key, A will no longer do the query $-Delegate$.

Challenge. A gives C a challenge identity vector $\vec{I}^*$. The restriction is that none of its prefix vectors has been inquired in phase 1. C randomly selects $\nu \in \{0,1\}$.

If $\nu = 0$, the challenger calculates $Encap(PK, \vec{I}) \to (C, k)$.

If $\nu = 1$, the challenger calculates $Encap*(PK, \vec{I}) \to C$.

The challenger sends the ciphertext C to the adversary.

Phase 2. It is similar with phase 1. The basic limitation is that any inquired identity vector cannot be a prefix of $\vec{I}^*$.

Guess. This adversary outputs a guess ν' about ν. If $\nu = \nu'$, A wins the game. This adversary's advantages are defined as $\text{Game}_{\text{Real}} Adv_A(\lambda) = |\Pr[\text{A wins}] - \frac{1}{2}|$. We have $\text{Game}_{\text{Real}} Adv_A(\lambda) \le \varepsilon$.

3) Smoothness

If $C \leftarrow Encap*(PK, \vec{I})$, $k \leftarrow Decap(PK, SK_{\vec{I}}, C)$ and $k' \leftarrow U$ (U is a uniform distribution), it can be get that $STDS((C,k),(C,k')) \le \varepsilon$.

IV. The Proposed LR-HIBE Scheme

A leakage-resistent and hierarchical identity-based encryption (LR-HIBE) scheme is given in this paper. The ciphertext is compressed to constant group elements and the private key can be re randomized by completely depending on the private key delegation algorithm. By BG-CO, we designs our the scheme. This private key is randomized by G_{v_3}. G_{v_2} is not used for the real system, but only as a semi-functional form.

Setup. This algorithm chooses a BG-CO G_1 and $N = v_1 v_2 v_3$, where v_1, v_2 and v_3 are different primes with the equal length. Let ℓ indicate the maximum depth for LR-HIBE. It randomly selects $g_1, h_1, u_1, \in G_{v_1}, X_3 \in G_{v_3}$ and $\alpha, \beta \in Z_N$. This public parameter is $PK = \{g_1, h_1, u_1, X_3, e(g_1,g_1)^{\alpha}, e(g_1,g_1)^{\beta}\}$. The master key is $MK = (g_1^{\alpha}, g_1^{\beta})$.

KeyG. It randomly selects $r, t \in Z_N$ and $R_3, R_3', R_3'' \in G_{v_3}$. It takes the public parameter and one identity vector $(ID_1, ..., ID_j)$ as input. It sets the private key:

$$K_1 = g_1^r R_3, K_2 = g_1^{\alpha} g_1^{-\beta t} (u_1^{ID_1 + ... + ID_j} h_1)^r R_3', K_3 = t, E = u_1^r R_3''.$$

Delegate. Given this private key K_1', K_2', E' for an identity vector $(ID_1, ..., ID_j)$ and an identity ID_{j+1}, this algorithm generates one private key based on this identity vector $(ID_1, ..., ID_j, ID_{j+1})$. It randomly selects $r', t' \in Z_N$ and $\tilde{R}_3, \tilde{R}', \tilde{R}'' \in G_{p_3}$ and gives the private key:

$$K_1 = K_1' g_1^{r'} \tilde{R}_3,$$
$$K_2 = K_2' g_1^{-\beta t'} (u_1^{ID_1 + ... + ID_j} h_1)^{r'} (E')^{ID_{j+1}} u_1^{r' ID_{j+1}} \tilde{R}_3',$$
$$K_3 = t', E = E' u_1^{r'} \tilde{R}''.$$

The new private key is completely randomized.

Encrypt. Given one message M and an identity vector $(ID_1, ..., ID_j)$, this algorithm randomly selects $s, d \in Z_N$. It computes the ciphertext:

$$C_0 = M \cdot Ext(e(g_1,g_1)^{\alpha s}, d), C_1 = (u_1^{ID_1 + ... + ID_j} h_1)^s,$$
$$C_2 = g_1^s, C_3 = e(g_1,g_1)^{\beta s}, C_4 = d$$

Decrypt. If one identity vector corresponding to a private key is just a prefix of $(ID_1, ..., ID_j)$, this algorithm runs the delegation algorithm to generate an identity vector corresponding to the ciphertext. Otherwise, when the private key and ciphertext for the identity vector $(ID_1, ..., ID_j)$, this algorithm gets the message as follows.

$$\frac{e(K_2,C_2)}{e(K_1,C_1)}C_3^{K_3}=\frac{e(g_1^{\alpha}g_1^{-\beta t}(u_1^{ID_1+...+ID_j}h_1)^r R_3^{'},g_1^s)}{e(g_1^r R_3,(u_1^{ID_1+...+ID_j}h_1)^s)}e(g_1,g_1)^{\beta st}$$

$$=\frac{e(g_1,g_1)^{\alpha s}e(u_1^{ID_1+...+ID_j}h_1,g_1)^{rs}}{e(g_1,u_1^{ID_1+...+ID_j}h_1)^{rs}}$$

$$=e(g_1,g_1)^{\alpha s}$$

$$C_0\oplus Ext(e(g_1,g_1)^{\alpha s},C_4)$$

$$=M\oplus Ext(e(g_1,g_1)^{\alpha s},d)\oplus Ext(e(g_1,g_1)^{\alpha s},d)=M$$

The security of our scheme can be obtained through the next game Game_{Real} which is played by the attacker and the challenger.

Game_{Real}.

Initialize. The challenger C runs the algorithm **Setup** to generate the public parameter PK for the attacker A. Let S denote the private key created by the challenger but not given to the attacker. The S is null at the beginning, i.e., $S=\phi$.

Phase 1. A can ask these oracles $-Create$, $-Delegate$, $-SK$, and leakage query ($-LK$).

$-Create$. A gives one identity vector $\vec{I}$. C calls the **KeyG** algorithm to obtain a private key and adds it in S. C only sends A a reference about the private key, not this private key itself.

$-Delegate$. A gives a private key $SK_{\vec{I}}$ in S and an identity ID. C connects ID and $\vec{I}$ to obtain $\vec{I}:ID$. Then, C generates a corresponding private key by calling the private key delegation algorithm. C only sends A a reference about the private key, not this private key itself.

$-SK$. A selects a specific element in S. C sends the private key to A. Then, C deletes it out of S. As for the private, A will no longer do the query $-Delegate$.

$-LK$. Given a private key $SK_{\vec{I}}$ for one identity vector $\vec{I}$, A can adaptively select the leakage function $f(\cdot)$. C returns $f(SK_{\vec{I}})$ to A. This output length for $f(SK_{\vec{I}})$ is recorded as ξ.

Challenge. The adversary gives C two challenge messages M_0 and M_1, and one identity vector $\vec{I}^*$. This identity vector must meet the condition that none of its prefix vectors is queried at phase 1. C randomly selects $\nu\in\{0,1\}$, calculates the ciphertext M_{υ} and sends it to A.

Phase 2. It is similar to phase 1. The extra constraint is that any inquired identity vector cannot be a prefix about $\vec{I}^*$.

Guess. A outputs a guess ν' about ν. If $\nu=\nu'$, A wins.

If any probability polynomial time adversary can only achieve negligible advantages in the game Game_{Real}, the given **LR-HIBE** is secure.

This proposed scheme is divided into two aspects. The first aspect is the proof of security. The second aspect is the analysis of leakage resilience. The details are given in the next section.

V. Safety Proof and Leakage Resilience Analysis

In general, the system presented in this study can be constructed through two steps. The first step is a key encapsulation algorithm (KEA), and the second step is to combine the extractor with the key encapsulation algorithm to construct our scheme. First, we prove that this KEA can constitute a hash proof system, which proves the security of our scheme. Then, by combining this obtained hash proof system with the extractor we get the proposed scheme. Thus, the leakage resilience performance can be analyzed according to the characteristics of the extractor.

A. Safety Proof

The presented LR-HIBE includes a key encapsulation algorithm. This key encapsulation algorithm is as follows.

Setup. This algorithm is identical with **Setup** algorithm of LR-HIBE.

KeyG. This algorithm is identical with **KeyG** algorithm of LR-HIBE.

Delegate. It is identical with **Delegate** algorithm of LR-HIBE.

Encap. $Encap(PK,\vec{I})\rightarrow(C,k)$. This algorithm inputs this public parameter PK and one identity vector $\vec{I}=(ID_1,...,ID_j)$, and randomly selects $s\in Z_N$. It outputs an invalid ciphertext $C=(C_1,C_2,C_3)=((u_1^{ID_1+...+ID_j}h_1)^s,g_1^s,e(g_1,g_1)^{\beta s})$.

The encapsulated key is $k=e(g_1,g_1)^{\alpha s}$.

Encap*. $Encap*(PK,\vec{I})\rightarrow C$. It inputs PK and one identity vector $\vec{I}$ and randomly selects $s,s'\in Z_N$. It outputs an invalid ciphertext.

$$C=(C_1,C_2,C_3)=((u_1^{ID_1+...+ID_j}h_1)^s,g_1^s,e(g_1,g_1)^{\beta s'}).$$

This algorithm is only used for the security proof.

Decap. $Decap(PK, SK_{\vec{I}}, C) \to k$. The algorithm inputs the ciphertext C and one private key $SK_{\vec{I}}$. It generates the encapsulated key $k = \frac{e(K_2, C_2)}{e(K_1, C_1)} C_3^{K_3}$.

We will prove that the key encapsulation algorithm is an HIB-HPS.

Proof.

1) Correctness: The decapsulation of a valid ciphertext is as follows.

$$\frac{e(K_2, C_2)}{e(K_1, C_1)} C_3^{K_3} = \frac{e(g_1^{\alpha} g_1^{-\beta t} (u_1^{ID_1+...+ID_j} h_1)^r R_3', g_1^s)}{e(g_1^r R_3, (u_1^{ID_1+...+ID_j} h_1)^s)} e(g_1, g_1)^{\beta st}$$

$$= \frac{e(g_1, g_1)^{\alpha s} e(u_1^{ID_1+...+ID_j} h_1, g_1)^{rs}}{e(g_1, u_1^{ID_1+...+ID_j} h_1)^{rs}}$$

$$= e(g_1, g_1)^{\alpha s}$$

So the correctness is established.

2) Smoothness: The decapsulation of a invalid ciphertext is as follows.

$$\frac{e(K_2, C_2)}{e(K_1, C_1)} C_3^{K_3} = \frac{e(g_1^{\alpha} g_1^{-\beta t} (u_1^{ID_1+...+ID_j} h_1)^r R_3', g_1^s)}{e(g_1^r R_3, (u_1^{ID_1+...+ID_j} h_1)^s)} e(g_1, g_1)^{\beta s' t}$$

$$= \frac{e(g_1, g_1)^{\alpha s} e(u_1^{ID_1+...+ID_j} h_1, g_1)^{rs}}{e(g_1, u_1^{ID_1+...+ID_j} h_1)^{rs}} e(g_1, g_1)^{\beta(s'-s)t}$$

$$= e(g_1, g_1)^{\alpha s} e(g_1, g_1)^{\beta(s'-s)t}$$

Because s and s' are randomly selected, $e(g,g)^{\alpha s} e(g,g)^{\beta t(s-s')}$ is evenly distributed in G_T . Thus, the smoothness is proved.

3) The indistinguishablitity between the valid and invalid ciphertext: First, we give the semi functional (SF) ciphertext and SF private key. They only play a role in proof.

SF ciphertext. Suppose that g_2 is a generator for G_{v_2} .Given the normal ciphertext C_1, C_2, C_3, this algorithm randomly selects $x, z_c \in Z_N$ and sets semi functional ciphertext $C_1' = C_1 g_2^{xz_c}, C_2' = C_2 g_2^{x}, C_3' = C_3$.

SF private key. First, this algorithm gains one normal private key K_1, K_2, K_3, E . Then, it randomly selects $\gamma, z_k, z \in Z_N$. It computes SF private key $K_1' = K_1 g_2^{\gamma}, K_2' = K_2 g_2^{\gamma z_k}, K_3' = K_3, E' = E g_2^{\gamma z}$.

When an SF private key decrypts an SF ciphertext, we have

$$\frac{e(K_2', C_2')}{e(K_1', C_1')} C_3'^{K_3'} = \frac{e(K_2 g_2^{\gamma z_k}, C_2 g_2^{x})}{e(K_1 g_2^{\gamma}, C_1 g_2^{xz_c})} C_3^{K_3}$$

$$= \frac{e(K_2, C_2)}{e(K_1, C_1)} C_3^{K_3} \frac{e(g_2^{\gamma z_k}, g_2^{x})}{e(g_2^{\gamma}, g_2^{xz_c})}$$

$$= e(g_1, g_1)^{\alpha s} \frac{e(g_2^{\gamma z_k}, g_2^{x})}{e(g_2^{\gamma}, g_2^{xz_c})} = e(g_1, g_1)^{\alpha s} e(g_2, g_2)^{x\gamma(z_k - z_c)}$$

It has an extra item $e(g_2, g_2)^{x\gamma(z_k - z_c)}$. When $z_c = z_k$, the decryption is correct. We call the semi functional private key a nominal SF private key.

This indiscernibility between the valid and invalid ciphertext can be achieved by constructing these games. Game_{Real} is a real security game. The ciphertext is generated by a valid encapsulation algorithm and is normal. $\mathrm{Game}_{Real'}$ is similar to Game_{Real} , but for all private key queries it generates the private key by calling the **KeyG** algorithm instead of using a delegation algorithm. $\mathrm{Game}_{\mathrm{Re}stricted}$ is similar to $\mathrm{Game}_{Real'}$, but an attacker cannot ask for such one identity that is the prefix for a challenge identity mode p_2 . Similar restrictions are set forth below. Let q indicate this number about inquiries.

Game_i ($i \in [0, q]$). It is similar to $\mathrm{Game}_{\mathrm{Re}stricted}$. The difference is that this ciphertext sent to an adversary is one SF cihertext. These forward i private keys are SF ones. These rearward private keys are normal ones. It Game_0 , only this ciphertext is SF form. In Game_q , this challenge ciphertext is SF one and every private key is SF one.

Game_{Semi} . It is similar to Game_q . The difference is that this challenge ciphertext is an SF invalid one which is generated by an invalid encapsulation algorithm.

Game_i' ($i \in [0, q]$). This game and Game_i are similar. The difference is that this ciphertext is generated by **Encap*** algorithm. For Game_0' , every private key is normal, and this ciphertext is SF and invalid. For Game_q' , all private keys except the first i queries are semi functional. This ciphertext is also SF and invalid.

Game_{Final} . This game and Game_{Real} are similar. The only difference is C chooses one normal and invalid ciphertext to A , i.e. he selects $\upsilon = 1$.

The following 7 lemmas prove the indiscernibility of this series of games.

Lemma 1. For every A, $\text{Game}_{\text{Real}}\, Adv_A = \text{Game}_{\text{Real'}}\, Adv_A$.

Proof. No matter a private key is generated by this private key delegation algorithm or by this private key generation algorithm, their distributions are identical. In the view of the adversary, they are not fundamentally different.

Lemma 2. If there is an adversary A that makes $\text{Game}_{\text{Real'}}\, Adv_A - \text{Game}_{\text{Restricted}}\, Adv_A = \varepsilon$, we may construct an algorithm C to destroy hypothesis 2 with more than $\frac{\varepsilon}{2}$ advantages.

Proof. Given g_1, X_1X_2, X_3, Y_2Y_3, C and A simulate $\text{Game}_{Real'}$. A can generate identity vector ID and ID^* over ε probability under the conditions that $ID \neq ID^* \bmod N$ and $(ID - ID^*)$ is divided by v_2. C obtains one nontrivial factor for N by calculating $x = \gcd(ID - ID^*, N)$. Let $y = \frac{N}{x}$. Because x is divided by v_2 and $N = xy = v_1v_2v_3$. There are three cases.

(1) x or y is v_1. Another one is v_2v_3.

(2) x or y is v_2. Another one is v_1v_3.

(3) x or y is v_3. Another one is v_1v_2.

For case 1, C determines which of x and y is the identity element through judging which of $(Y_2Y_3)^x$ and $(Y_2Y_3)^y$ is the identity element. In general, it can be assumed that $x = v_1$ and $y = v_2v_3$. C determines whether T contains G_{v_2} part through testing whether $e(T^x, X_1X_2)$ is an identity element. If not, T has the G_{v_2} composition.

For case 2, C tests which of $(X_1X_2)^x$ and $(X_1X_2)^y$ is the identity element. If none of them is the identity element and it is not case 1, it is case 2. C determines which of x and y is v_1v_3 through testing which of g_1^x and g_1^y is an identity element. In general, it can be assumed that $x = v_2$ and $y = v_1v_3$. C determines whether T contains G_{v_2} part through testing whether T^y is an identity element. If T^y is an identity element, $T \in G_{v_1v_3}$. If not, T has the G_{v_2} composition ($T \in G_1$).

If case 1 and case 2 do not holds, case 3 holds. By detecting which of X_3^x and X_3^y is the identity element, C determines which of x and y is v_3. Without losing generality, it can be assumed that $x = v_3$. C determines whether T contains G_{v_2} part through judging whether $e(T^x, Y_2Y_3)$ is an identity element. If not, T contains G_{v_2} composition. Thus, the algorithm B destroys hypothesis 2 with more than $\frac{\varepsilon}{2}$ advantages.

Lemma 3. If there exists an algorithm A who makes $\text{Game}_{\text{Restricted}}\, Adv_A - \text{Game}_0\, Adv_A = \varepsilon$. We may construct an algorithm C to destroy hypothesis 1 with more than $\frac{\varepsilon}{2}$ advantages.

Proof. Given g_1, X_3, T, C simulates the $\text{Game}_{\text{Restricted}}$ or Game_0 with A. C randomly selects $\alpha, a, b \in Z_N$, and sets $u_1 = g_1^a$ and $h_1 = g_1^b$. C sends the public parameter $\{N, g_1, h_1, u_1, e(g_1, g_1)^\alpha\}$ to A. When C is requested to provide a private key corresponding to the identity vector $\vec{I}_j = (ID_1, ..., ID_j)$, he randomly selects $r, t, t', w, v \in Z_N$, and calculates: $K_1 = g_1^r X_3^t, K_2 = g^\alpha (u_1^{ID_1 + ... + ID_j} h_1)^r X_3^w, K_3 = t', E = u_1^r X_3^v$. C generates the normal ciphertext $C = (C_1, C_2, C_3) = (T^{a(ID_1^* + ... + ID_j^*) + b}, T, e(T, g_1)^\beta)$.

This implies that g_1^s is a part for T. If $T \in G_{v_1v_2}$, this is an SF ciphertext, where $z_c = a(ID_1^* + ... + ID_j^*) + b$. A simulates Game_0. If $T \in G_{v_1}$, this is a normal ciphertext. A simulates $\text{Game}_{\text{Restricted}}$. Thus, the algorithm C destroys hypothesis 1 with more than $\frac{\varepsilon}{2}$ advantages.

Lemma 4. If there exists an algorithm A who makes $\text{Game}_{i-1}\, Adv_A - \text{Game}_i\, Adv_A = \varepsilon$. We may construct an algorithm C to destroy hypothesis 2 with more than $\frac{\varepsilon}{q}$ advantages.

Proof. The algorithm C needs to select an identity vector to create an SF private key. C does not know the challenge identity vector before the challenge phase, so C randomly

selects one as the challenge identity vector. The probability of success is $\frac{1}{q}$. Given g_1, X_1X_2, X_3, Y_2Y_3 and T, C randomly selects $\alpha, a, b \in Z_N$. C obtains the public parameters $u_1 = g_1^a, h_1 = g_1^b, e(g_1, g_1)^\alpha$ and sends them to A. When A queries a private key of the p^{th} ($p < i$) identity vector $(ID_1, ..., ID_j)$, C generates an SF private key. C randomly selects $r, z, t, t', v \in Z_N$. C computes $K_1 = g_1^r (Y_2Y_3)^t, K_2 = g_1^\alpha (u_1^{ID_1+...+ID_j} h_1)^r (Y_2Y_3)^z, K_3 = t', E = u_1^r (Y_2Y_3)^v$. This is an SF private key, where $g_2^\gamma = Y_2^t$.

When $p > i$, C calls the normal **KeyG** generation algorithm to achieve a normal private key.

In order to generate the private key of the p^{th} identity vector $(ID_1, ..., ID_j)$, C sets $z_c = a(ID_1^* + ... + ID_j^*) + b$. C randomly selects $w_k, w \in Z_N$, and calculates $K_1 = T, K_2 = g_1^\alpha T^{z_k} X_3^{w_k}, K_3 = t', E = T^a X_3^w$.

Supposing that $T \in G_{v_1 v_3}$, this private key is normal, where g_1^r is equal to this G_{v_1} part about T. If $T \in G_1$, this is an SF private key.

Challenge. A selects an identity vector ID^* = $(ID_1^*, ..., ID_j^*)$ and gives it to C. C terminates if C cannot guess the private key correctly. Otherwise, C calculates the ciphertext as follows: $(C_1, C_2, C_3) = ((X_1X_2)^{a(ID_1^*+...+ID_j^*)+b}, X_1X_2, e(X_1X_2, g_1)^\beta)$, where $g_1^s = X_1$ and $z_k = a(ID_1^* + ... + ID_j^*) + b$. Since the i^{th} identity is not the prefix about ID^* modulo v_2, z_c and z_k are randomly distributed in A 's view. This relationship of z_c and z_k is crucial. When C tests whether the i^{th} private key is semi functional, he creates an SF ciphertext about ID^*, and decrypts it. Regardless of whether this i^{th} private key is semi functional, decryption can always succeed for $z_c = z_k$. In fact, this is equivalent to creating a nominal semi functional private key.

If $T \in G_{v_1 v_3}$, C simulates Game_{i-1} correctly. If $T \in G_1$, C simulates Game_i correctly. Thus, C destroys hypothesis 2 with more than $\frac{\varepsilon}{q}$ advantages.

Lemma 5. Supposing that there exists an algorithm A that makes $\text{Game}_q Adv_A - \text{Game}_{Semi} Adv_A = \varepsilon$. We may construct one algorithm C to destroy hypothesis 3 with more than $\frac{\varepsilon}{q}$ advantages.

Proof. Given $g_1, g_1^\beta X_2, X_3, g_1^s Y_2, Z_2, T$, C randomly selects $\alpha, a, b, t^*, \tilde{\alpha} \in Z_N$ such that $\alpha = t^* \beta + \tilde{\alpha}$ and sets the public parameters

$$u_1 = g_1^a, h_1 = g_1^b, e(g_1, g_1)^\beta = e(g_1 X_2, g_1)^\beta,$$
$$e(g_1, g_1)^\alpha = (e(g_1, g_1)^\beta)^{t^*} e(g_1, g_1)^{\tilde{\alpha}},$$

and sends them to A.

When A queries the private key of the identity vector $(ID_1, ..., ID_j)$, C randomly selects one to generate an SF private key for C is not aware of the challenge identity vector. The probability of success is $\frac{1}{q}$. C selects $c, r, t, z, z', w, w' \in Z_N$ at random and computes

$$K_1 = g_1^r Z_2^z X_3^t, K_2 = (g_1^\beta X_2)^{\tilde{t}} g_1^{\tilde{\alpha}} (u_1^{ID_1+...+ID_j} h_1)^r X_3^w Z_2^c,$$
$$K_3 = t^* - \tilde{t}, E = u_1^r Z_2^{z'} X_3^{w'}.$$

It is a properly distributed SF private key, where $(g_1^\beta)^{\tilde{t}} g_1^{\tilde{\alpha}} = g_1^\alpha g_1^{-\beta K_3'}$.

A selects the challenge identity vector ID^* = $(ID_1^*, ..., ID_j^*)$ and gives it to C. C selects $r, t, w, z, w' \in Z_N$ at random and generates a properly distributed normal private key

$$K_1^* = g_1^r X_3^t, K_2^* = g_1^{\tilde{\alpha}} (u_1^{(ID_1+...+ID_j)} h_1)^r X_3^w,$$
$$K_3^* = t^*, E = u_1^r Z_2^{z'} X_3^{w'}.$$

A gives C $ID^* = (ID_1^*, ..., ID_j^*)$. C gives the ciphertext $(C_1, C_2, C_3) = ((g_1^s Y_2)^{a(ID_1^*+...+ID_j^*)+b}, g_1^s Y_2, T)$ to A, Let $z_c = a(ID_1^* + ... + ID_j^*) + b$. z_c is modulo v_2 and $u_1 = g_1^a$ and $h_1 = g_1^b$ are some elements of G_{v_1}. If $\alpha, a, b \in Z_N$ are selected randomly, $\alpha, a, b \in Z_N$ modulo N is not related to $z_c = a(ID_1^* + ... + ID_j^*) + b$ modulo v_2.

In the event that $T = e(g_1, g_1)^{as}$, this ciphertext is a properly distributed SF ciphertext. In the event that $T \in G_2$, this is an SF ciphertext about one random message. So, the algorithm C destroys hypothesis 3 with more than $\frac{\varepsilon}{q}$ advantages.

Lemma 6. Supposing that there exists an algorithm A that makes $\text{Game}_i^{'} Adv_A - \text{Game}_{i-1}^{'} Adv_A = \varepsilon$. We may construct one algorithm C to destroy hypothesis 2 with more than $\frac{\varepsilon}{2}$ advantages.

Proof. This process of proof is similar to that of Lemma 4.

Lemma 7. Supposing that there exists an algorithm A that makes $\text{Game}_1^{'} Adv_A - \text{Game}_{Final} Adv_A = \varepsilon$. We may construct one algorithm C to destroy hypothesis 3 with more than $\frac{\varepsilon}{2}$ advantages.

Proof. This process of proof is similar to that of Lemma 5.

Theorem 1. If hypothesis 1, hypothesis 2 and hypothesis 3 are true, the valid ciphertext and invalid ciphertext are indistinguishable.

Proof. The maximum advantages obtained by the adversary in hypothesis 1, hypothesis 2 and hypothesis 3 are respectively denoted by $\varepsilon_1, \varepsilon_2$ and ε_3.

According to the above 7 lemmas, the difference between the advantages of adversary A in the above different games are:

$$\text{Game}_{\text{Real}'} Adv_A - \text{Game}_{Restricted} Adv_A \le \varepsilon_2,$$

$$\text{Game}_{Restricted} Adv_A - \text{Game}_0 Adv_A \le \varepsilon_1,$$

$$\text{Game}_{i-1} Adv_A - \text{Game}_i Adv_A \le q\varepsilon_2,$$

$$\text{Game}_q Adv_A - \text{Game}_{Semi} Adv_A \le q\varepsilon_3,$$

$$\text{Game}_i^{'} Adv_A - \text{Game}_{i-1}^{'} Adv_A \le q\varepsilon_2,$$

$$\text{Game}_1^{'} Adv_A - \text{Game}_{Final} Adv_A \le q\varepsilon_3,$$

From the above inequality, we can get.

$$\text{Game}_{\text{Real}'} Adv_A - \text{Game}_{Final} Adv_A \le \varepsilon_2 + \varepsilon_1 + 2q(q-1)\varepsilon_2 + 2q\varepsilon_3 .$$

Because the above equation is a polynomial about q, any adversary's advantage can be ignored.

B. Performance Analysis about Leakage Resilience

Based on the key encapsulation algorithms: Setup, KeyG, Delegate, Encap, Encap*, and Decap, our LR-HIBE scheme is constructed. The encapsulated key space has $Log(p_1)$ elements. We use a $(Log(p_1) - Leak, \varepsilon)$ strong extractor $Ext: \{0,1\}^{lop(v_1)-Leak} \times \{0,1\}^r \to \{0,1\}^{lop(v_1)}$. The obtained LR-HIBE has the same algorithm as the key encapsulation algorithms: Setup, KeyG, Delegate. The encryption and decryption algorithms are as follows.

Encrypt: $\text{Encrypt}(PK, M, \vec{I}) \to CT$. This algorithm calls $\text{Encap}(PK, \vec{I}) \to (C, k)$, randomly selects a seed s^* of the extractor and sets $C_0 = Ext(k, s^*) \oplus M$. This algorithm generates a ciphertext $CT = (C_0, s^*, C)$, where $C = (C_1, C_2, C_3)$.

Decrypt: $\text{Decrypt}(PK, CT, SK_{\vec{I}}) \to \text{M}$. It takes PK, CT and $SK_{\vec{I}}$ as the input, where $CT = (C_0, s^*, C)$ and $k = Decap(C, SK_{\vec{I}})$. It outputs the message $M = Ext(k, s^*) \oplus C_0$. The decryption can succeed as long as the identity vector used in decryption is the same as the identity vector used by this encryption.

Theorem 2. If there is a key encapsulation algorithm as defined in section 4.1. By the above transformation we can get LR-HIBE (that is, the scheme given in this paper). This relative leakage ratio about the encapsulated key of this given LR-HIBE is close to 1.

Proof. Let $View$ represent the view (all random variables) that A sees when there is no leakage, we have $\tilde{H}_\infty(A|View) = LogN$. The encapsulated key length is $LogN$. When there is a leakage query, adversary A can obtain ξ bits information which is regarded as $Leak$, that is, $Leak$ has 2^ξ values. According to conclusion 1 we get $\tilde{H}_\infty(A|Leak, View) \ge \tilde{H}_\infty(A|View) - \xi = LogN - \xi$. Therefore, as long as the extractor is $(LogN - \xi, \varepsilon)$ strong, $SD((Ext(k, s*), s*, Leak, View), (U, s*, Leak, View)) \le \varepsilon$, where U is uniformly distributed. As long as the performance of the extractor is good enough, this leakage amount ξ for an encapsulated key is close to $LogN$. So the distance of $C_0 = Ext(k, s^*) \oplus M$ and the uniform distribution is ε. Thus, this statistical distance about two ciphertexts is no more than 2ε. Consequently, no PPT adversary may make a distinction between two challenge ciphertexts over more than 2ε advantage. This relative leakage ratio is $\rho = Leak / LogN \approx LogN / LogN = 1.$

Theorem 2 is proved.

VI. Performance Comparisons and Experimental Simulation

Some comparisons between this study and several related researches [6, 8] are given in Table I. LR stands for leakage resilience. $|G_{v_1}|$ and $|G_{v_3}|$ represent the element length of the subgroup G_{p_1} and G_{p_3}, respectively. E indicates exponential operation in the group.

We make some comparisons about leakage resilience, public key length, private key generation and encryption cost. Our scheme has the same public key length, private key generation, private key delegation, and encryption costs as [8]. This public key in our scheme is much smaller than that given in [6], which greatly reduces the network communication burden. Since the number of system layers in a hierarchy can generally reach ten or more, the computation cost of our scheme for private key generation and private key delegation is much lower than that of the scheme [6]. When the number of layers is little, the encryption cost of our scheme is basically the same as theirs, but when the number of layers gradually increases, our encryption calculation operation is obviously better than that given in [6].

TABLE I. Some Comparisons between Our Scheme and Several Related Schemes [6, 8]

	[8]	[6]	Ours
LR	No	No	Yes
Public Key Size	$3\|G_{v_1}\|+\|G_{v_3}\|$	$(l+2)\|G_{v_1}\|+\|G_{v_3}\|$	$3\|G_{v_1}\|+\|G_{v_3}\|$
Private Key Generation	$5E$	$(l+3)E$	$5E$
Private Key Delegation	$6E$	$(l+3)E$	$6E$
Encryption	$4E$	$(j+3)E$	$4E$

In addition to the performance comparisons, we also give the experimental simulation.

The experimental platform is a PC with 64 bit operating system Windows 10, 3.40 GHz main frequency, 8.00G RAM and Intel (R) Core (TM) i7-6700 CPU. Based on Java Pairing Based Cryptography Library 2.0.0 [43], we use Eclipse 4.4.1 for simulation software. A 160 bit composite order elliptic curve $y^2 = x^3 + x$ is selected for our experiment. The private key generation time is 0.125 seconds, the private key delegation time is 0.150 seconds, and the encryption time is 0.100 seconds.

VII. Conclusions

We propose a hierarchal and efficient identity-based encryption scheme. This given scheme may resist the bounded leakage for this encapsulated key. By using dual system encryption combined with hash proof system, the security proof can be achieved. The leakage resilient function is realized by using extractor technology. The relative leakage ratio of the encapsulated key is close to 1.

The features of this scheme are as follows.

1) There is no limit to the hierarchy depth of the system, and only the maximum hierarchy length is required to be given when the system is initialized.

2) The system has the performance of resisting the leakage of encapsulated symmetric keys, and the relative leakage rate of encapsulated symmetric keys can almost reach 1.

3) The system is efficient, because unnecessary parameters are appropriately reduced.

The scheme in this study is constructed in composite order groups, and the computational cost may be slightly higher than that is constructed in prime order groups. In the future, we will start to consider how to construct an LR encryption scheme in prime order groups.

Attribute based encryption is a generalization of identity based encryption and has good applications. How to construct efficient and leakage resilient attribute based encryption is worth further study.

Acknowledgment

This research was funded by the National Natural Science Foundation of China (grant numbers: 62172292, 62072104, 61972095, U21A20465).

References

[1] D. Pavithran, J. N. Al-Karaki, and K. Shaalan, "Edge-based blockchain architecture for event-driven IoT using hierarchical identity based encryption," *Inform. Process. Manag.* vol. 58, no. 3, Article ID 102528, 2021, https://doi.org/10.1016/j.ipm.2021.102528.

[2] C. L. Fan, C. H. Shie, Y. F. Tseng, and H. C. Huang, "An efficient data protection scheme based on hierarchical ID-based encryption for MQTT," *Acm. T. Sensor. Network.* vol. 19, no. 3, pp. 1-21, 2023.

[3] C. Gentry, and A. Silverberg, "Hierarchical ID-based cryptography," In Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, 1-5 December, 2002.

[4] J. Horwitz, and B. Lynn, "Toward hierarchical identity-based encryption," In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2002, Amsterdam, The Netherlands, 28 April- 2 May 2002.

[5] D. Boneh, X. Boyen, and E. Goh, "Hierarchical identity based encryption with constant size ciphertext," In Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2005, Aarhus, Denmark, 22-26 May 2005.

[6] A. Lewko, and B. Waters, "New techniques for dual system encryption and fully secure hibe with short ciphertexts," In Proceedings of the 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, 9-11 February 2010.

[7] J. Chen, and H. Wee, "Dual system groups and its applications compact HIBE and more," Cryptology ePrint Archive, 2014, https://eprint.iacr.org/2014/265.

[8] L. Guo, J. Wang, and W. C.Yau, "Efficient hierarchical identity-based encryption system for internet of things infrastructure," Symmetry, vol. 11, no. 7, Article ID 913, 2019, https://doi.org/10.3390/sym11070913.

[9] D. Kalyani, and R. Sridevi, "New hierarchical identity based encryption with maximum hierarchy," Int. J. Netw. Secur. vol. 21, no. 1, pp. 40-46, 2019.

[10] X. F. Jiang, T. Wang, and Z. W. Sun, "Chosen-ciphertext secure hierarchical identity-based encryption from R-LWE," J. Comput. vol. 31, no. 1, pp. 320-331, 2020.

[11] K, Emura, A. Takayasu, and Y. Watanabe, "Efficient identity-based encryption with hierarchical key-insulation from HIBE," Design. Code. Cryptogr. vol. 89, pp. 2397-2431, 2021.

[12] Y. Okano, J. Tomida, A. Nagai, K. Yoneyama, and A. Fujioka, et al. "Revocable hierarchical identity-based authenticated key exchange," In Proceedings of the International Conference on Information Security and Cryptology, ICISC 2021, Seoul, Korea, 1-3 December 2021.

[13] G. Song, Y. Deng, Q. Huang, C. Peng, and C. Tang, "Hierarchical identity-based inner product functional encryption," Inform. Sciences. vol. 573, pp. 332-344, 2021.

[14] R. Langrehr, and J. Pan, "Tightly secure hierarchical identity-based encryption," J. Cryptol. vol. 33, pp. 1787-1821, 2020.

[15] G. Srivastava, R. Agrawal, K. Singh, R. Tripathi, and K. Naik, "A hierarchical identity-based security for delay tolerant networks using lattice-based cryptography," Peer. Peer. Netw. Appl. vol. 13, pp. 348-367, 2020.

[16] J. Shikata, and Y. Watanabe, "Identity-based encryption with hierarchical key-insulation in the standard model," Design. Code. Cryptogr. vol. 87, no. 5, pp. 1005-1033, 2019.

[17] J. Gong, Z. Cao, S. Tang, and J. Chen, "Extended dual system group and shorter unbounded hierarchical identity based encryption," Design. Code. Cryptogr. vol. 80, pp. 525-559, 2016.

[18] L. Zhang, Y. Mu, and Q. Wu, "Compact anonymous hierarchical identity-based encryption with constant size private keys," Comput. J. vol. 59, no. 4, pp. 452-461, 2016.

[19] W. Liu, J. Liu, Q. Wu, B. Qin, and Y. Li, "Practical chosen-ciphertext secure hierarchical identity-based broadcast encryption," Int. J. Inf. Secur. vol. 15, pp. 35-50, 2016.

[20] D. Jauvart, N. El Mrabet, J. J. Fournier, and L. Goubin, "Improving side-channel attacks against pairing-based cryptography," J. Cryptogr. Eng. vol. 10, pp. 1-16, 2020.

[21] T. Weng, T. Cui, T. Yang, and Y. Guo, "Related-key differential attacks on reduced-round LBlock," Secur. Commun. Netw. vol. 2022, Article ID 8464960, 2022, https://doi.org/10.1155/2022/8464960.

[22] G. de Souza Faria, and H. Y. Kim, "Differential audio analysis: a new side-channel attack on PIN pads," Int. J. Inf. Secur. vol. 18, pp. 73-84, 2019.

[23] C. S. Chen, T. Wang, and J. Tian, "Improving timing attack on RSA-CRT via error detection and correction strategy," Inform. Sciences. vol. 232, pp. 464-474, 2013.

[24] M. Naor, and G. Segev, "Public-key cryptosystems resilient to key leakage," Siam. J. Comput. vol. 41, no. 4, pp. 772-814, 2012.

[25] Z. Brakerski, Y. T. Kalai, J. Katz, and V. Vaikuntanathan, "Overcoming the hole in the bucket: Public-key cryptography resilient to continual memory leakage," In Proceedings of the 51st Annual Symposium on Foundations of Computer Science. Las Vegas, NV, USA, 23-26 October 2010.

[26] J. Li, Q. Yu, and Y. Zhang, "Identity-based broadcast encryption with continuous leakage resilience," Inform. Sciences. vol. 429, pp. 177-193, 2018.

[27] H. Hou, B. Yang, M. Zhang, Y. Zhou, and M. Huang, "Fully secure wicked identity-based encryption resilient to continual auxiliary-inputs leakage," J. Inf. Secur. Appl. vol. 53, Article ID 102521, 2020.

[28] J. Li, M. Teng, Y. Zhang, and Q. Yu, "A leakage-resilient CCA-secure identity-based encryption scheme," Comput. J. vol. 59, no. 7, pp. 1066-1075, 2016.

[29] A. Lewko, Y. Rouselakis, and B. Waters, "Achieving leakage resilience through dual system encryption," In Proceedings of the 8th Theory of Cryptography Conference, TCC 2011, Providence, RI, USA, 28-30 March 2011.

[30] J. Li, Q. Yu, Y. Zhang, and J. Shen, "Hierarchical attribute based encryption with continuous leakage-resilience," Inform. Sciences. vol. 484, pp. 113-134, 2019.

[31] Y. Guo, J. Li, Y. Zhang, and J. Shen, "Hierarchical attribute-based encryption with continuous auxiliary inputs leakage," Secur. Commun. Netw. vol. 9, no. 18, pp. 4852-4862, 2016.

[32] Y. Guo, Z. Lu, M. Jiang, and D. Zhang, "Ciphertext-policy attribute-based encryption against post-challenge continuous auxiliary inputs leakage," Int. J. Netw. Secur. vol. 24, no. 3, pp. 511-520, 2022.

[33] Y. Zhou, Y. Xu, Z. Qiao, B. Yang, and M. Zhang, "Continuous leakage-resilient certificate-based signcryption scheme and application in cloud computing," Theor. Comput. Sci. vol. 860, pp. 1-22, 2021.

[34] Q. Yu, J. Li, and Y. Zhang, "Leakage-resilient certificate-based encryption," Secur. Commun. Netw. vol. 8, no. 18, pp. 3346-3355, 2015.

[35] Q. Yu, J. Li, and Y. Zhang, "Certificate-based encryption resilient to key leakage," J. Syst. Software. vol. 116, pp. 101-112, 2016.

[36] Y. Zhou, B. Yang, H. Cheng, and Q. Wang, "A leakage-resilient certificateless public key encryption scheme with CCA2 security," Front. Inform. Tech. El. vol. 19, pp. 481-493, 2018.

[37] Y. M. Tseng, S. S. Huang, T. T. Tsai, Y. H. Chuang, and Y. H. Hung, "Leakage-resilient revocable certificateless encryption with an outsourced revocation authority," Informatica-Lithuan. vol. 33, no. 1, pp. 151-179, 2022.

[38] D. Boneh, E. J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," In Proceedings of the second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, 10-12 February 2005.

[39] N. Nisan, and D. Zuckerman, "Randomness is linear in space," J. Comput. Syst. Sci. vol. 52, no. 1, pp. 43-52, 1996.

[40] Y. Dodis, R. Ostryovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," Siam. J. Comput. vol. 38, no. 1, pp. 97-139, 2008.

[41] L. Zhang, J. Zhang, Y. Mu, "Novel leakage-resilient attribute-based encryption from hash proof system," Comput. J. vol. 60, no. 4, pp. 541-554, 2016.

[42] Q. Q. Lai, B. Yang, Y. Yu, Z. Xia, Y. Zhou, et al. "Updatable identity-based hash proof system based on lattices and its application to leakage-resilient public-key encryption schemes," J. Comput. Sci. Tech-CH. vol. 33, pp. 1243-1260, 2018.

[43] A. De,Caro, and V. Iovino, "jPBC: Java pairing based cryptography," In Proceedings of the 2011 IEEE symposium on computers and communications (ISCC), Kerkyra, Greece, 28 June 2011 - 01 July 2011.