A Novel Hierarchical Identity-Based Encryption Scheme from Lattices

Qing Ye, Mingxing Hu, Wei Gao, and Yongli Tang(✉)

College of Computer Sciences and Technology, Henan Polytechnic University,
Jiaozuo 454000, Henan, China
yltang@hpu.edu.cn

Abstract. Hierarchical identity based encryption is a powerful public key encryption scheme where entities are arranged in a directed tree. Each entity in the tree is provided with a secret key from its parent and can delegate this secret key to its children so that a child entity can decrypt messages intended for it. Aiming at the high complexity in user's private key extraction and large expansion ratio of trapdoor size in previous hierarchical identity-based encryption schemes, in this paper, we proposed a new HIBE scheme. We first used the implicit extension method to improve preimage sampling algorithm, and then we combined the improved algorithm with MP12 trapdoor delegation algorithm to construct an efficient hierarchical identity-based encryption user's private key extraction algorithm. Finally, we integrated the new extraction algorithm and the Dual-LWE algorithm to complete our scheme. Compared with the similar schemes, the efficiency of our scheme is improved in system establishment and user's private key extraction stage, the trapdoor size grows only linearly with the system hierarchical depth, and the improved preimage sample algorithm partly solves the Gaussian parameter increasing problem induced by MP12 trapdoor delegation. The security of the proposed scheme strictly reduces to the hardness of decisional learning with errors problem in the standard model.

Keywords: Lattice · Hierarchical Identity-Based encryption
Trapdoor function · Learning with errors

1 Introduction

Hierarchical identity-based encryption (HIBE) system [1, 2] is the extend version of identity-based encryption (IBE) [3–6], in the IBE cryptosystem, a single KGC can't meet in a large-scale network generated identity key for each user independently, because in a large number of user requests. To verify complete identity information for each user and for the establishment of private key security transfer channel is quite occupied system resources. Therefore, a hierarchical identity based encryption system is needed to complete the above problems. In the HIBE system, multiple KGC entities are distributed according to the structure of the directed tree. One of its characteristics is that each KGC trapdoor in the system is specified by its father KGC, which is called the

X. Sun et al. (Eds.): ICCCS 2018, LNCS 11065, pp. 412–422, 2018.
https://doi.org/10.1007/978-3-030-00012-7_38

trapdoor derivation. It should be noted that the trapdoor derivation is one-way, which means that each sub-KGC can't use its trapdoor to restore the parent KGC trapdoor.

In recent years, based on the new cryptosystem lattice theory because of its good asymptotic efficiency, simple operation, can be parallelized, anti-attack and quantum worst-case random instances has become a research hotspot after the era of quantum cryptography, and [7–11] made a series of achievements. In 2010, Cash et al. [12] Eurocrypt 10 proposed a trapdoor derivative algorithm, and this algorithm is based on lattice structure's first HIBE program, the program will be the identity of the user as consisting of a series of bits for each bit allocation and a uniform random matrix, which will lead to increased number of dimensional lattice with grading system the depth of significant growth, and the proposed algorithm derived trapdoor trapdoor derived size and depth is two times the classification system of power relations in the growth, high grade depth HIBE system will appear in the trapdoor size is too large and lead to the problem of normal. In addition, the scheme uses Gentry to [13] et al. STOC'08 proposed preimage sampling algorithm, the preimage sampling algorithm needs to perform high precision real orthogonal iteration, leads to the complexity of the user key extraction. The same year, Agrawal et al. [14] in Eurocrypt 10 to Cash et al's scheme is improved, will be in accordance with the user identity vector of each bit allocation matrix is improved by way of classification system in each stage of a distribution matrix, so that the lattice dimension only increases linearly with the depth of the grading system growth. But the trapdoor derivative algorithm and preimage sampling algorithm is still not changed, and the complexity of the trapdoor key size has not been fundamentally improved the extraction of user.

Micciancio et al. [15] (hereinafter referred to as MP12) in Eurocrypt'12 proposed a new lattice trapdoor generation algorithm and the corresponding preimage sampling algorithm, compared to the previous generation of trapdoor trapdoor generation algorithm [16], the process is simple, the complexity is equivalent to only two of a random matrix multiplication, and does not involve the high computation cost of HNF (Hermite normal form) and matrix inversion operation. Compared to the previous preimage sampling algorithm [13, 17], MP12 algorithm is relatively simple, preimage sampling algorithm, and support parallel computing and input for small integers, on line space demand is low. In addition, Micciancio et al. proposed trapdoor derived a new algorithm, the algorithm is compared with Cash et al. [12] algorithm is more efficient, because the algorithm does not need to Gauss sampling values are linearly independent detection, and the elimination of the ToBasis and HNF operation, more important is the size and grading system derived trapdoor depth only linearly growth. But at the same time, we note that the derived MP12 algorithm also has some shortcomings, the largest singular quality derived trapdoor trapdoor and derivative derivative algorithm compared to before the trapdoor trapdoor that matrix value will increase, resulting in the deterioration of the quality of the trapdoor, which led to a series of problems such as the growth parameters of Gauss. So using MP12 preimage sampling algorithm and trapdoor derivative algorithm to construct HIBE scheme, there will be a user key low extraction complexity and smaller size of the trapdoor expansion rate, but also should pay attention to avoid the growth of Gauss parameters derived from MP12 algorithm in the structure problem of the HIBE program. To optimize the preimage sampling algorithm using the implicit Cash method proposed by [12] et al. extended to a certain extent, can solve this problem, and can avoid unnecessary calculation and reduce the time complexity of the algorithm preimage sampling. Gentry et al. [13] pointed out that in the construction of HIBE scheme, the dual LWE algorithm should be used to complete the encryption and decryption stage of the scheme, which is more reasonable than the non-dual LWE algorithm. Subsequently, HIBE scheme [19–22] based on dual LWE algorithm has been proposed.

In order to make the HIBE scheme more practical and feasible, we must solve the problem of the complexity of user key extraction algorithm and the expansion rate of trapdoor size. Therefore, this paper proposes a new HIBE scheme on grid. The main contributions are: (1) to improve the MP12 preimage sampling algorithm in the HIBE scheme using implicit method, solves the Gauss parameters of the trapdoor derived after preimage sampling algorithm will increase the problem; (2) the improved preimage sampling algorithm and MP12 algorithm are combined to derive the trapdoor, construct a HIBE algorithm to extract the user key, and combined with dual LWE algorithm HIBE program structure. The security model is verified by the same security model similar to the same scheme. The proof results show that under the standard model, the security of the scheme can be reduced to the decisional learning with errors problem (DLWE).

2 Preliminaries

2.1 Lattice and Gaussian Distribution

Given n linearly independent vectors $\boldsymbol{B} = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$, a lattice Λ generated by $\boldsymbol{B}$ is defined as $\Lambda = \left\{\boldsymbol{Bk} = \sum_{i \in [n]} k_i \cdot \boldsymbol{b}_i : \boldsymbol{k} \in \mathbb{Z}^n\right\}$. We call $\boldsymbol{B}$ as basis of Λ. In this paper, our schemes work with a special class of integer lattices. Let $n \geq 1$ and modulus $q \geq 2$ be integers, where n is the main security parameter throughout this work, and all other parameters are implicitly functions of n. An m-dimensional lattice from the family is specified relative to the additive group $\mathbb{Z}_q^n$ by a parity check matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$. The associated lattice is defined as follows:

$$\begin{aligned} \Lambda^{\perp}(\boldsymbol{A}) &= \{\boldsymbol{x} \in \mathbb{Z}^m : \boldsymbol{Ax} = 0 \bmod q\} \\ \Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A}) &= \{\boldsymbol{x} \in \mathbb{Z}^m : \boldsymbol{Ax} = \boldsymbol{u} \bmod q\} \end{aligned} \tag{1}$$

Note that $\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A})$ is a coset of $\Lambda^{\perp}(\boldsymbol{A})$.

For $\boldsymbol{y} \in \Lambda$, any $\sigma > 0$ and dimension $m \geq 1$, the Gaussian function $\rho_{\sigma,\boldsymbol{c}} : \mathbb{R}^m \to (0, 1]$ centered at $\boldsymbol{c} \in \mathbb{R}^m$ is defined as $\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{y}) = \exp\left(-\pi\|\boldsymbol{y} - \boldsymbol{c}\|^2/\sigma^2\right)$. Let $\rho_{\sigma,\boldsymbol{c}}(\Lambda) = \sum_{\boldsymbol{y} \in \Lambda} \rho_{\sigma,\boldsymbol{c}}(\boldsymbol{y})$, and define the discrete Gaussian distribution over Λ as $D_{\Lambda,\sigma,\boldsymbol{c}}(\boldsymbol{y}) = \frac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{y})}{\rho_{\sigma,\boldsymbol{c}}(\Lambda)}$.

2.2 The Learning with Errors Problem

Security of all our schemes reduces to the LWE (learning with errors) problem, a classic hard problem on lattices defined by Regev [7].

Definition 1 [7]: Consider these public parameters: a prime q, a positive integer n, and a distribution χ over $\mathbb{Z}_q$. An $(\mathbb{Z}_q, n, \chi)$-LWE problem instance is a challenge oracle $\mathcal{O}$ which consists of access to two types oracle, either, a noisy pseudo-random oracle $\mathcal{O}_s$ carrying some constant random secret key $\boldsymbol{s} \in \mathbb{Z}_q^n$, or, a truly random oracle $\mathcal{O}_\$$, whose behaviors are respectively described as follows:

$\mathcal{O}_s$: outputs samples of the form $(\boldsymbol{u}_i, v_i) = (\boldsymbol{u}_i, \boldsymbol{u}_i^T \boldsymbol{s} + x_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, where $\boldsymbol{s} \in \mathbb{Z}_q^n$ is a uniformly distributed persistent value invariant across invocations, $\boldsymbol{u}_i$ is uniform in $\mathbb{Z}_q^n$, and $x_i \in \mathbb{Z}_q$ is a fresh sample from χ.

$\mathcal{O}_\$$: outputs truly uniform random samples from $\mathbb{Z}_q^n \times \mathbb{Z}_q$.

The $(\mathbb{Z}_q, n, \chi)$-LWE problem allows repeated queries to the challenge oracle $\mathcal{O}$. We define that an attack algorithm $\mathcal{A}$ distinguishes the $(\mathbb{Z}_q, n, \chi)$-LWE problem if $\text{LWE - adv}[\mathcal{A}] = \left|\Pr\left[\mathcal{A}^{\mathcal{O}_s} = 1\right] - \Pr\left[\mathcal{A}^{\mathcal{O}_\$} = 1\right]\right|$ is non-negligible for a random $\mathbf{s} \in \mathbb{Z}_q^n$.

3 Algorithm Design and Scheme Construction

3.1 Optimized HIBE Preimage Sampling Algorithm

The implicit extension of preimage sampling algorithm of HIBE in [15] were optimized, and then the trapdoor derivative algorithm and Lemma 2 combined to construct an efficient HIBE algorithm to extract the user key.

Theorem 1. *According to the conclusion of the 1 trapdoor derivative algorithm Lemma 2 the existence of Gauss parameter growth problems in the trapdoor derivation, the implicit method can be extended to optimize the Gauss parameters σ' in the preimage sampling process, and avoids the computation and storage of the derived matrix $\boldsymbol{R}'$.*

Proof. The output of MP12 derived known trapdoor $\boldsymbol{R}' \in \mathbb{Z}_q^{m \times w}$ is not full rank matrix, compared to before the trapdoor expansion pie $\boldsymbol{R} \in \mathbb{Z}_q^{\bar{m} \times w}$ matrix dimension $m - \bar{m}$, maximum singular $s_1(\boldsymbol{R}') > s_1(\boldsymbol{R})$ and trapdoor trapdoor quality matrix, the relationship between Gauss parameters and trapdoor quality $s_1(\boldsymbol{R}) \cdot \omega(\sqrt{\log n})$, therefore $\sigma' > \sigma$, the time complexity of the algorithm preimage sampling $\boldsymbol{v} \leftarrow \mathit{SampleL}(\boldsymbol{R}', \boldsymbol{u}', \sigma')$ for trapdoor dimension expansion and derivative significantly, and Gauss parameters σ' of the growth of output norm vector algorithm becomes large. The implicit extension method can effectively solve the above problems. The concrete algorithms are as follows:

The matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$ and the trapdoor matrix $\boldsymbol{R} \in \mathbb{Z}_q^{\bar{m} \times w}$ of the TrapGen algorithm in the Lemma 1 are sum, the extended matrix of the matrix $\boldsymbol{A}$, which is a homogeneous random matrix $\boldsymbol{A}' = [\boldsymbol{A} || \bar{\boldsymbol{A}}] \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^{n \times w}$. It is the trapdoor matrix $\bar{\boldsymbol{A}} \in \mathbb{Z}_q^{n \times w}$ of the matrix $\boldsymbol{R}' \in \mathbb{Z}_q^{m \times w}$ output by the DelTrap algorithm in Lemma 2. An algorithm $\mathcal{O}(\boldsymbol{a}, \sigma')$

for generating a vector, which is used to generate random and non-distinguishable vectors from the distribution $D_{\mathbb{Z}^w,\sigma'}$ statistics.

(1) Generation $\bar{\boldsymbol{v}} \leftarrow \mathcal{O}(\boldsymbol{a}, \sigma')$, judgment $\bar{\boldsymbol{v}}$ and statistical $D_{\mathbb{Z}^w,\sigma'}$ proximity, if not, then regenerate;
(2) Calculation $\bar{\boldsymbol{u}} = f_{\bar{A}}(\bar{\boldsymbol{v}}) = \square\boldsymbol{A}\bar{\boldsymbol{v}} \in \mathbb{Z}_q^n$;
(3) Execute the algorithm $\boldsymbol{v} \leftarrow SampleL(\boldsymbol{R}, \boldsymbol{u}' - \bar{\boldsymbol{u}}, \sigma)$, output $\boldsymbol{v}' = \boldsymbol{v}||\bar{\boldsymbol{v}}$.

Because the output $\mathcal{O}(\boldsymbol{a}, \sigma)$ is random, the non-homogeneous small integer solutions (ISIS, inhomogeneous small integer solution problem) is found to be statistically uniform, then by Theorem 3 in [15] shows the output vector preimage sampling algorithm is statistically homogeneous, therefore is also statistically uniform.

3.2 Efficient HIBE Identity Key Extraction Algorithm

This section uses MP12 optimization preimage trapdoor derivative algorithm and sampling algorithm described in Sect. 3.2 are combined to construct a efficient HIBE user key extraction algorithm. The algorithm mainly completes the HIBE user key extraction operation in the scheme.

Algorithm. The identity-key extracting algorithm for HIBE HIBE - ExtractSK (MPK,$\boldsymbol{A}_{\boldsymbol{id}_{\ell-1}}, \boldsymbol{R}_{\ell-1}, (\boldsymbol{id}_1||\ldots||\boldsymbol{id}_{\ell-1})||\boldsymbol{id}_\ell)$

Input. The master public key MPK, matrix $\boldsymbol{A}_{\boldsymbol{id}_{\ell-1}} \in \mathbb{Z}_q^{n\times[m+(\ell-1)w]}$, trapdoor matrix $\boldsymbol{R}_{\ell-1} \in \mathbb{Z}^{\bar{m}(\ell-1)\times w}$ and identity $(\boldsymbol{id}_1||\ldots||\boldsymbol{id}_{\ell-1})||\boldsymbol{id}_\ell \in \mathbb{Z}_q^{\ell n}$.

Output. Identity key $\boldsymbol{e}_{\boldsymbol{id}_\ell}$.

(1) Using the FRD (full-rank differences) function [14], the user identity $\boldsymbol{id}_\ell$ is mapped into a matrix $\boldsymbol{H}_{id_\ell}$, $\boldsymbol{A}_{\boldsymbol{id}_\ell} = [\boldsymbol{A}_{\boldsymbol{id}_{\ell-1}}||\boldsymbol{A}_\ell + \boldsymbol{H}_{\boldsymbol{id}_\ell}\boldsymbol{G}]$ which is a homogeneous random matrix $\boldsymbol{A}_\ell$.
(2) Implementation of trapdoor derivative algorithm $\boldsymbol{R}_\ell \leftarrow DelTrap^{\mathcal{O}}(\boldsymbol{A}' = [\boldsymbol{A}_{\boldsymbol{id}_{\ell-1}}|| \boldsymbol{A}_\ell + \boldsymbol{H}_{\boldsymbol{id}_\ell}\boldsymbol{G}], \boldsymbol{H}_\ell, \sigma_\ell)$, the details of the algorithm is the use of discrete Gauss distribution in Oracle $\mathcal{O}$ lattice coset $\Lambda^\perp(\boldsymbol{A})$ and Gauss parameters σ_ℓ is suitable on independent sampling, sampling results as a column vector of trapdoor matrix $\boldsymbol{R}_\ell$, and finally meet $\boldsymbol{A}_{\boldsymbol{id}}\boldsymbol{R}_\ell = \boldsymbol{H}_\ell\boldsymbol{G} - (\boldsymbol{A}_\ell + \boldsymbol{H}_{\boldsymbol{id}_\ell}\boldsymbol{G})$.
(3) After the execution optimization in Sect. 3.2 preimage sampling algorithm $\boldsymbol{e}_{\boldsymbol{id}_\ell} \leftarrow SampleL(\boldsymbol{R}_\ell, \boldsymbol{u}_\ell, \sigma_\ell)$, which $\sigma_\ell = s_1(\boldsymbol{R}) \cdot \omega(\sqrt{\log \ell n})$ meet $\boldsymbol{A}_{\boldsymbol{id}_\ell} \cdot \boldsymbol{e}_{\boldsymbol{id}_\ell} = \boldsymbol{u}_\ell$ and $||\boldsymbol{e}_{\boldsymbol{id}_\ell}|| \leq \sigma_\ell\sqrt{m + \ell w}$, output $\boldsymbol{e}_{\boldsymbol{id}_\ell}$.

By Lemma 1 and the definition of FRD function [14] algorithm shows the first step of the matrix $[\boldsymbol{A}_\ell + \boldsymbol{H}_{\boldsymbol{id}_\ell}\boldsymbol{G}]$ is uniform random, by Lemma 2 shows that algorithm second step trapdoor matrix $\boldsymbol{R}_\ell$ derived to satisfy the unidirectional, by Theorem 3 in [14] shows that the output distribution of discrete Gauss dative third step preimage sampling algorithm, $\Lambda_{\boldsymbol{u}}^\perp(\boldsymbol{A}')$ are statistically indistinguishable.

With the HIBE grading depth increase, MP12 trapdoor trapdoor derived algorithm output size dimensions $\Lambda^\perp(\boldsymbol{A}')$ only dative linear growth relationship, rather than a power of two growth relations, linear independence and without trapdoor derived detection without high computational cost, operation ToBasis and HNF operation. To sum up, the user key extraction algorithm combined with the Sect. 3.2 algorithm is safe and feasible, and has lower time complexity and trapdoor size expansion.

3.3 HIBE Construction

In order to solve the problem of the complexity of user key extraction algorithm and the expansion rate of trapdoor size in HIBE scheme, we should start with the system establishment and user key extraction stage. The former mainly depends on the complexity of the trapdoor generation algorithm, the main complexity of the latter depends on the trapdoor derivation and preimage sampling algorithm. Compared with the existing lattice HIBE scheme of [12, 14, 19, 22], the characteristics of the scheme is first proposed by MP12 et al. the trapdoor generation, preimage sampling and trapdoor derivative algorithm to construct a scheme to enhance the system establishment and the user key extraction stage performance and efficiency; and the first method using implicit extended optimized sampling algorithm on MP12 preimage. As for the encryption and decryption phase of this scheme, the dual LWE algorithm is still used, similar to the other HIBE scheme [12, 14, 19, 22].

The concrete scheme is constructed as follows, including its basic parameters: uniform random matrix $\boldsymbol{A}_0 \in \mathbb{Z}_q^{n\times m}$ and the trapdoor $\boldsymbol{R}_0 \in \mathbb{Z}^{\bar{m}\times w}$, which n is safe and is supported by the system parameters, d is the maximum depth classification, user identity $\boldsymbol{id} = (\boldsymbol{id}_1||\ldots||\boldsymbol{id}_\ell)$, $1 \le \ell \le d$, and among them $\boldsymbol{id}_i \in \mathbb{Z}_q^n \backslash \{0\}$, $i \in [1, \ell]$, a structure $\boldsymbol{G} = \boldsymbol{I}_n \otimes \boldsymbol{g}^T \in \mathbb{Z}_q^{n\times nk}$, which is the unit matrix $\boldsymbol{I}_n$, FRD function $H : \mathbb{Z}_q^n \to \mathbb{Z}_q^{n\times n}$.

HIBE - Setup$(1^n, d)$: Input security parameters 1^n and system maximum classification depth d, run algorithm TrapGen$(1^n, q)$, output even random matrix $\boldsymbol{A}_0 \in \mathbb{Z}_q^{n\times m}$ and $\boldsymbol{A}_0$ trapdoor matrix $\boldsymbol{R}_0 \in \mathbb{Z}_q^{\bar{m}\times w}$, and select a uniform random matrix $s_1(\boldsymbol{R}_0) \le O(\sqrt{n \log q}) \cdot \omega(\sqrt{\log n})$, select dimension uniform random vector, output main public key MPK $= (\boldsymbol{A}_0, \boldsymbol{A}_1, \ldots, \boldsymbol{A}_d, \boldsymbol{G}, \boldsymbol{u})$ and main private key MSK $= \boldsymbol{R}_0 \in \mathbb{Z}_q^{\bar{m}\times w}$.

HIBE - Extract$(\text{MPK}, \boldsymbol{R}_{\ell-1}, (\boldsymbol{id}_1||\ldots||\boldsymbol{id}_{\ell-1})||\boldsymbol{id}_\ell)$: Enter the main public key MPK, user identity $\boldsymbol{id}_\ell \in \mathbb{Z}_q^n$, $\mathbf{R}_{\ell-1}$ which represents the trapdoor corresponding to the user's public key matrix $\mathbf{A}_{\boldsymbol{id}_{\ell-1}}$ when the system classifying depth is $\ell - 1$, then $\boldsymbol{A}_{\boldsymbol{id}_{\ell-1}} = [\boldsymbol{A}_0||\boldsymbol{A}_1 + \boldsymbol{H}_{id_1}\boldsymbol{G}||\boldsymbol{A}_2 + \boldsymbol{H}_{id_2}\boldsymbol{G}||\ldots||\boldsymbol{A}_{\ell-1} + \boldsymbol{H}_{id_{\ell-1}}\boldsymbol{G}]$, the user key extraction algorithm HIBE - ExtractSK$(\text{MPK}, \boldsymbol{A}_{\boldsymbol{id}_{\ell-1}}, \boldsymbol{R}_{\ell-1}, (\boldsymbol{id}_1||\ldots||\boldsymbol{id}_{\ell-1})||\boldsymbol{id}_\ell)$ of the Sect. 3.3 is invoked, and the user key $\boldsymbol{e}_{id_\ell}$ is output.

HIBE - Encrypt$(\text{MPK}, \boldsymbol{id}, b)$: Input the main public key MPK, the user identity $\boldsymbol{id} = (\boldsymbol{id}_1||\ldots||\boldsymbol{id}_\ell)$ of the hierarchical depth ℓ and the message $b \in \{0, 1\}$ to be encrypted. A matrix $\boldsymbol{A}_{id_\ell} = [\boldsymbol{A}_0||\boldsymbol{A}_1 + \boldsymbol{H}_{id_1}\boldsymbol{G}||\boldsymbol{A}_2 + \boldsymbol{H}_{id_2}\boldsymbol{G}||\ldots||\boldsymbol{A}_\ell + \boldsymbol{H}_{id_\ell}\boldsymbol{G}] \in \mathbb{Z}_q^{n\times(m+\ell w)}$ is constructed, where $\boldsymbol{H}_{\boldsymbol{id}_i} \leftarrow H(\boldsymbol{id}_i)$ a uniform random vector $\boldsymbol{s} \leftarrow \mathbb{Z}_q^n$ and a uniform random matrix $\bar{\boldsymbol{R}} \leftarrow \{-1, 1\}^{m\times \ell w}$ are selected, and the fault tolerance $x \xleftarrow{\bar{\Psi}_\alpha} \mathbb{Z}_q$, fault-tolerant vector $\boldsymbol{y} \xleftarrow{\bar{\Psi}_\alpha^m} \mathbb{Z}_q^m$, $\boldsymbol{z} = \bar{\boldsymbol{R}}^T \boldsymbol{y} \in \mathbb{Z}_q^{\ell w}$ and output ciphertext $\boldsymbol{CT} = (c_0, \boldsymbol{c}_1) \in \mathbb{Z}_q \times \mathbb{Z}_q^{m+\ell w}$ are calculated.

HIBE - Decrypt(MPK,$\boldsymbol{e}_{\boldsymbol{id}_\ell}$, $\boldsymbol{CT}$): Enter the main public key MPK, ciphertext $\boldsymbol{CT} = (c_0, \boldsymbol{c}_1)$ and user key $\boldsymbol{e}_{\boldsymbol{id}_\ell}$, calculate $b' = c_0 - \boldsymbol{e}_{\boldsymbol{id}_\ell}^T \boldsymbol{c}_1 \in \mathbb{Z}_q$, and compare b' with the integers $\lfloor q/2 \rfloor$ in the view $\mathbb{Z}$, if, output 1, otherwise output 0.

4 Security Proof

Agrawal et al. [14] INDr-sID-CPA security model lattice HIBE scheme in Eurocrypt 10 the standard model security proof by using the scheme, based on the security model of security proof and Yang et al. in 2014 [19] and 2016 Wang et al. [22] proposed HIBE scheme.

4.1 HIBE Correctness

The noise bound is the same as that of the document [14] HIBE scheme. The upper bound is $q\ell^2\sigma_\ell m\alpha_\ell \cdot \omega(\sqrt{\log m}) + O\left(\ell^2\sigma_\ell m^{3/2}\right)$ to ensure that the system is running effectively and the noise is less than $q/5$ that in the document $1 \leq \ell \leq d$, we set the parameters as follows. The correctness of the proposed scheme is clearly established if we set m=$2n \log q$, σ_ℓ=$w \cdot \omega(\sqrt{\log n})$, α_ℓ=$[wm \cdot \omega(\sqrt{\log n})]^{-1}$ and q=$w\sqrt{m^3} \cdot \omega(\sqrt{\log n})$.

4.2 Security Reduction

Theorem 2 Supposing that the LWE problem described in Definition 1 is hard under the parameters $(m, \sigma_\ell, \alpha_\ell, q)$ setting as is shown in Sect. 4.1, the proposed HIBE scheme is provable INDr-sID-CPA secure in the standard model.

Proof. The proof of theorem is used to prove the method that based on the sequence of games, used W_i to define the attacker Game i in the correct guess challenge bit events, namely, in the end, $r \in \{0, 1\}$ which is used as the random bit Challenger decided to challenge ciphertext types, $r' \in \{0, 1\}$ is speculation stage at the end of the game, the output of the attacker's bit challenge guess the solution, PPT proved that for any adversary to challenge the advantage of zero bit guess, an attacker cannot win with non negligible advantage in INDr-sID-CPA Game. The DLWE problem is used to prove that Game2 and Game3 are not distinguishable.

Game 0. Game 0 is a INDr-sID-CPA game between an attacker and a challenger to attack this program.

Game 1. The Game 1 is set $\boldsymbol{id}^* = \left(\boldsymbol{id}_1^* || \ldots || \boldsymbol{id}_k^*\right)$ as an attacker to be attacked, if $k < d$ the zero vector $(d-k)$ is supplemented in the spare part. The generation mode of the change $\boldsymbol{A}_1, \ldots, \boldsymbol{A}_d$ is selected, and a random matrix $\boldsymbol{R}_1^*, \ldots, \boldsymbol{R}_d^* \leftarrow \{-1, 1\}^{m \times w}$ is selected and the structure matrix is constructed $\boldsymbol{A}_i = \left[-\boldsymbol{H}_{id_i^*} \cdot \boldsymbol{G} - \boldsymbol{A}_0 \boldsymbol{R}_i^*\right]$. Set up to use to generate challenge ciphertext at the challenge stage. It is found that the $\bar{\boldsymbol{R}}_k^* = \left(\boldsymbol{R}_1^* || \ldots || \boldsymbol{R}_k^*\right) \in \{-1, 1\}^{m \times kw}$ distribution $(\boldsymbol{A}_0, \boldsymbol{A}_0 \boldsymbol{R}^*, \boldsymbol{z})$ and distribution $\left(\boldsymbol{A}_0, \boldsymbol{A}_1', \boldsymbol{z}\right)$ of the Lemma 4 in [14] can not be distinguished from the statistics, including the homogeneous matrix and the random matrix $\boldsymbol{R}^* \in [-1,1]^{m \times kw}$. So the matrix $\boldsymbol{A}_1,\ldots,\boldsymbol{A}_d$ is statistically non - distinguishable in Game1 and Game0, and the attacker seems to be the same in Game0 and Game1.

Game 2. The difference between Game 2 and Game1 lies in the use of the TrapGen algorithm to generate the trapdoor matrix $\boldsymbol{G} \in \mathbb{Z}_q^{n \times w}$ of the matrix $\boldsymbol{R_G}$ in Game2, and $\boldsymbol{A}_i = \left[-\boldsymbol{H}_{id_i^*} \cdot \boldsymbol{G} - \boldsymbol{A}_0\boldsymbol{R}_i^*\right]$ still remains the form in Game1. Query the user key response to the attacker, the attacker needs to set the query identity $\boldsymbol{id} = (\boldsymbol{id}_1||\ldots||\boldsymbol{id}_\ell)$, the output matrix $\boldsymbol{A_{id}}$ of the trapdoor matrix, which $\boldsymbol{A_{id}} = [\boldsymbol{A}_1||\ldots||\boldsymbol{A}_\ell||\boldsymbol{A}_{\ell+1}] + [\boldsymbol{0}||\boldsymbol{H}_{\boldsymbol{id}_1} \cdot \boldsymbol{G}||\ldots||\boldsymbol{0}||\boldsymbol{H}_{\boldsymbol{id}_\ell} \cdot \boldsymbol{G}||\boldsymbol{0}] = [\boldsymbol{G}_{id} - \boldsymbol{A}_0\bar{\boldsymbol{R}}_\ell]$, $\bar{\boldsymbol{R}}_\ell = \left[\boldsymbol{R}_1^*||\ldots||\boldsymbol{R}_\ell^*\right] \in \mathbb{Z}_q^{m \times \ell w}$, $\boldsymbol{G}_{id} = \left[\left(\boldsymbol{H}_{\boldsymbol{id}_1} - \boldsymbol{H}_{\boldsymbol{id}_1^*}\right)\boldsymbol{G}||\ldots||\left(\boldsymbol{H}_{\boldsymbol{id}_\ell} - \boldsymbol{H}_{\boldsymbol{id}_\ell^*}\right)\boldsymbol{G}\right] \in \mathbb{Z}_q^{n \times \ell w}$ by definition, FRD encoding function [14] that $\left[\boldsymbol{H}_{\boldsymbol{id}_i} - \boldsymbol{H}_{\boldsymbol{id}_i^*}\right]$ is invertible matrix, it can use the trapdoor Challenger matrix in response to the attacker's preimage sampling private key query prefix $\boldsymbol{id}$, as defined by the security model know the query is not target identity of the attackers and, therefore, can use $\boldsymbol{e}_{\boldsymbol{id}_\ell} \leftarrow \mathrm{SampleR}(\boldsymbol{A}_0, \bar{\boldsymbol{R}}_\ell, \boldsymbol{G}_{id}, \boldsymbol{R_G}, \sigma_\ell)$ the Challenger trapdoor matrix in response to user key attacker preimage sampling query. If the algorithm is called, the output is sent to the attacker; if $\boldsymbol{id} \neq \boldsymbol{id}^*$ the $\left[\boldsymbol{H}_{\boldsymbol{id}_i} - \boldsymbol{H}_{\boldsymbol{id}_i^*}\right]$ zero matrix is irreversible, the game terminates and returns a random bit. It is known from the Theorem 4 in [14] that the distribution $\sigma_\ell > s_1(\boldsymbol{R}_\ell) \cdot \|\bar{\boldsymbol{R}}_\ell\| \cdot \omega(\sqrt{\log n})$ of the distribution in the Game1 can not be distinguished from the statistics. So the private key query response $\boldsymbol{e_{id}}$ method in Game2 and the matrix and Game1 are not statistically different, so the attacker's advantages in Game2 and Game1 are the same.

Game 3. The difference between the Game 3 and the Game2 is that the challenge ciphertext $\left(c_0^*, \boldsymbol{c}_1^*\right)$ is no longer generated by the encryption algorithm, but is selected from the ciphertext space $\mathbb{Z}_q \times \mathbb{Z}_q^{\ell w + m}$ independently and randomly. Because the challenge of ciphertext is a random selection, the advantage of an attacker can be ignored.

Next, using the difficulty of the DLWE problem, it is proved that for the PPT enemy, Game3 and Game2 are undistinguishable.

Assuming that a PPT opponent $\mathcal{A}$ can distinguish between Game2 and Game3, we use an enemy $\mathcal{A}$ to construct an algorithm $\mathcal{B}$ to solve the problem of DLWE. The simulator $\mathcal{B}$ has a series of samples $(\boldsymbol{u}_i, v_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, $i = 0, 1, \ldots, \bar{m}$. The enemy $\mathcal{A}$ announced $\mathcal{B}$ his identity id^* to the impersonator.

Setup. The simulator $\mathcal{B}$ generates random matrix $\boldsymbol{A}_0 \in \mathbb{Z}_q^{n \times m}$ by sample. The first row of the matrix $\boldsymbol{A}$ is vector $\boldsymbol{u}_i$. The sample vector is taken as a common random vector $\boldsymbol{u} \in \mathbb{Z}_q^n$, and the rest parameters are the same as those generated in Game2.

Query. Analogous to Game2, the simulator $\mathcal{B}$ generates a polynomial key for the enemy $\mathcal{A}$.

Challenge. The opponent $\mathcal{A}$ submits the information $b^* \in \{0,1\}$. The simulator $\mathcal{B}$ operates as follows: $v_0, v_1, \ldots, v_m$ representing a sample component in the DLWE problem, making the blind message bits $\boldsymbol{v}^* = \begin{bmatrix} v_1 \\ \vdots \\ v_m \end{bmatrix} \in \mathbb{Z}_q^m$, so that we can select the random bits $c_0^* = v_0 + b^* \cdot \lfloor q/2 \rfloor \in \mathbb{Z}_q$, $\boldsymbol{c}_1^* = \begin{bmatrix} \boldsymbol{v}^* \\ \left(-\bar{\boldsymbol{R}}_k^*\right)^T \boldsymbol{v}^* \end{bmatrix} \in \mathbb{Z}_q^{m+kw}$, if we send them to the opponents, if we choose them randomly, and send them to the opponents.

If the distribution in the DLWE problem is pseudorandom, then the $\boldsymbol{A}_{id^*} = \left[\boldsymbol{A}_0 || -\boldsymbol{A}_0 \bar{\boldsymbol{R}}_k^*\right]$ distribution is the same as that of Game2. At this point, it is known from the sample definition, $\boldsymbol{v}^* = \boldsymbol{A}_0^T \boldsymbol{s} + \boldsymbol{y}$ of which $\boldsymbol{y} \overset{\bar{\Psi}_\alpha^m}{\longleftarrow} \mathbb{Z}_q^m$. Therefore, the above definition is satisfied

$$\boldsymbol{c}_1^* = \begin{bmatrix} \boldsymbol{A}_0^T \boldsymbol{s} + \boldsymbol{y} \\ -\bar{\boldsymbol{R}}_k^{*T} \boldsymbol{A}_0^T \boldsymbol{s} - \bar{\boldsymbol{R}}_k^{*T} \boldsymbol{y} \end{bmatrix} = \begin{bmatrix} \boldsymbol{A}_0^T \boldsymbol{s} + \boldsymbol{y} \\ \left(-\boldsymbol{A}_0^T \bar{\boldsymbol{R}}_k^*\right)^T \boldsymbol{s} - \bar{\boldsymbol{R}}_k^{*T} \boldsymbol{y} \end{bmatrix} = (\boldsymbol{A}_{id^*})^T \boldsymbol{s} + \begin{bmatrix} \boldsymbol{y} \\ -\bar{\boldsymbol{R}}_k^{*T} \boldsymbol{y} \end{bmatrix}$$

The upper right side is the Game2's challenge ciphertext $v_0 = \boldsymbol{u}_0^{\mathrm{T}} \boldsymbol{s} + x$. It is also the satisfaction of the above definition, which is the $x \overset{\bar{\Psi}_\alpha}{\longleftarrow} \mathbb{Z}_q$ challenge of the Game2. If the distribution $c_0^* = \boldsymbol{u}_0^{\mathrm{T}} \boldsymbol{s} + x + b^* \lfloor q/2 \rfloor$ in the DLWE problem is really random, it is uniform in the upper and uniform in the upper. By the standard Left over hash Lemma [23], it is known that the above definition is independent and uniform $\boldsymbol{v}^*$. Therefore, the distribution of the challenge ciphertext is equally uniform $\mathbb{Z}_q \times \mathbb{Z}_q^{m+kw}$ in the Game3.

Guess. After the end of the polynomial sub-selective inquiry, the enemy $\mathcal{A}$ conjectures the interaction between Game2 or Game3. The conjecture $\mathcal{B}$ output of the simulator is used as a solution to the DLWE problem. Because there is no PPT algorithm to solve the DLWE problem effectively, this scheme is INDr-sID-CPA secure.

5 Conclusion

This paper presents a new lattice hierarchical identity based encryption scheme, the new scheme is based on the application of implicit method is extended to MP12 HIBE in the preimage sampling algorithm was improved to a certain extent to solve in combination with MP12 trapdoor algorithm derived Gauss parameters will increase in depression after birth of martial art, and saves unnecessary computation and storage. Then, an efficient HIBE user key extraction algorithm is constructed with MP12 trapdoor derivation algorithm. Finally, the HIBE scheme is constructed with dual LWE algorithm. Under the standard model, the security of the scheme can be reduced to the difficulty of the determinant fault-tolerant learning problem (DLWE), and a strict security proof is given. The comparative analysis shows that the efficiency of this scheme is better than that of the same scheme in the stage of system establishment and the user key extraction stage.

6 Acknowledgments

This work was supported by the “13th Five-Year” National Crypto Development Foundation (MMJJ20170122), the Project of science and Technology Department of Henan Province (142300410147), the Project of Education Department of Henan Province (12A520021, 16A520013), the Doctoral Fund of Henan Polytechnic University (B2014-044), the Natural Science Foundation of Henan Polytechnic University (No.T2018-1).

References

1. Gentry, C., Silverberg, A.: Hierarchical ID-based cryptography. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 548–566. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-36178-2_34
2. Horwitz, J., Lynn, B.: Toward hierarchical identity-based encryption. In: Knudsen, Lars R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 466–481. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-46035-7_31
3. Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44647-8_13
4. Lai, J., Deng, R.H., Liu, S., Weng, J., Zhao, Y.: Identity-based encryption secure against selective opening chosen-ciphertext attack. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 77–92. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55220-5_5
5. Yamada, S.: Adaptively secure identity-based encryption from lattices with asymptotically shorter public parameters. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016. LNCS, vol. 9666, pp. 32–62. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49896-5_2
6. Wang, F., Liu, Z., Wang, C.: Full secure identity-based encryption scheme with short public key size over lattices in the standard model. Proc. Int. J. Comput. Math. **93**(6), 854–863 (2016)
7. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM **56**(6), 84–93 (2009)
8. Nguyen, Phong Q., Zhang, J., Zhang, Z.: Simpler efficient group signatures from lattices. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 401–426. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46447-2_18
9. Brakerski, Z., Perlman, R.: Lattice-Based fully dynamic multi-key FHE with short ciphertexts. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9814, pp. 190–213. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53018-4_8
10. Libert, B., Ling, S., Nguyen, K., Wang, H.: Zero-knowledge arguments for lattice-based accumulators: logarithmic-size ring signatures and group signatures without trapdoors. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016. LNCS, vol. 9666, pp. 1–31. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49896-5_1
11. Duan, R., Gu, C., Zhu, Y.: Efficient identity-based fully homomorphic encryption over NTRU. J. Commun. **38**(1), 66–75 (2017)

12. Cash, D., Hofheinz, D., Kiltz, E., Peikert, C.: Bonsai trees, or how to delegate a lattice basis. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 523–552. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_27
13. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing, STOC 2008, Victoria, British Columbia, Canada, pp. 197–206. ACM (2008)
14. Agrawal, S., Boneh, D., Boyen, X.: Efficient lattice (H)IBE in the standard model. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 553–572. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_28
15. Micciancio, D., Peikert, C.: Trapdoors for lattices: simpler, tighter, faster, smaller. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 700–718. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_41
16. Alwen, J., Peikert, C.: Generating shorter bases for hard random lattices. Theor. Comput. Syst. **48**(3), 535–553 (2011)
17. Peikert, C.: An efficient and parallel gaussian sampler for lattices. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 80–97. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14623-7_5
18. Agrawal, S., Boyen, X., Vaikuntanathan, V., Voulgaris, P., Wee, H.: Functional encryption for threshold functions (or fuzzy IBE) from lattices. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 280–297. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-30057-8_17
19. Yang, C., Zheng, S., Wang, L., Lu, X., Yang, Y.: Hierarchical identity-based broadcast encryption scheme from LWE. J. Commun. Netw. **16**(3), 258–263 (2014)
20. Katsumata, S., Yamada, S.: Partitioning via non-linear polynomial functions: more compact IBEs from ideal lattices and bilinear maps. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10032, pp. 682–712. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53890-6_23
21. Zhang, J., Chen, Yu., Zhang, Z.: Programmable hash functions from lattices: short signatures and IBEs with small key sizes. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9816, pp. 303–332. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53015-3_11
22. Wang, F., Wang, C., Liu, Z.: Efficient hierarchical identity based encryption scheme in the standard model over lattices. Front. Inf. Technol. Electron. Eng. **17**(8), 781–791 (2016)
23. Dodis, Y., Ostrovsky, R., Reyzin, L., Smith, A.: Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. Proc. Soc. Ind. Appl. Math. (SIAM) **38**(1), 97–139 (2008)