Efficient Lattice based (H)IB-DRE

Kunwar Singh[1], C. Pandu Rangan[2], Ilsun You[3], Amalan Joseph Antony[1], SK Karthika[1], Jiyoon Kim[4*]

[1]National Institute of Technology, Tiruchirappalli, TamilNadu, India

[2]Indian Institute of Technology, Chennai, TamilNadu, India

[3]Kookmin University, Seoul, Republic of Korea
isyou@kookmin.ac.kr

[4]Gyeongsang National University, Jinju, Gyeongsangnam-do, Republic of Korea
jykim92@gnu.ac.kr

Received: August 31, 2022; Accepted: November 1, 2022; Published: December 31, 2022

Abstract

In CCS'04, Diament etc al. presented special kind of public key encryption called Dual Receiver Encryption (DRE). In DRE, sender encrypts the plaintext using public keys of two independent receivers. Both independent receivers can decrypt the ciphertext into the same plaintext using their own private keys. This new cryptography primitive has applications in construction of complete non-malleability and plaintext-awareness public key encryption, for a secure management of data that is to be disseminated to distributed processors, for ubiquitous and mobile computing applications. Daode Zhang et. al. constructed lattice-based IB-DRE scheme which is secure against stronger security notion i.e. adaptive-ID. We present hierarchical identity based dual encryption (HIB-DRE) scheme under LWE assumption. To the best of our knowledge, this gives the first provably secure HIB-DRE scheme in the lattice based setting. Independent work by Naccache[1] and Chatterjee - Sarkar[2] presented a variant of Waters's identity based encryption scheme to reduce Public Parameters. They have considered an identity of l-bits as l' chunks where size of each chunk is l/l'. This reduces the Public Parameter (PP) size from l to l' $n \times m$ matrices. This idea was named as blocking technique[3]. We have used blocking technique to reduce the size of PP. Daode Zhang et. al.[4] presented adaptive secure IB-DRE scheme. This scheme[4] contains $l+1$, $n \times m$ matrices as PPs, where l denotes the number of the bits in identity. Using blocking technique we have reduced the size of PP by around factor β. Because of this the size of prime number q in field Z_q is increased by 2^{β} which results in increase in computation cost. We have shown that compared to Daode Zhang et. al.scheme the size of the PP can be decreased approximately by 80% and the time complexity is increased by only 1.40% for a suitably chosen β.

Keyworkds: Lattice, identity based cryptosystem, Dual receiver encryption

1 Introduction

In CCS'04, Diament etc al.[5] presented special kind of public key encryption called Dual Receiver Encryption (DRE). In DRE, sender encrypts the message using public keys of two independent receivers.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 13(4):1-23, Dec. 2022
DOI:*10.58346/JOWUA.2022.I4.001*

*Corresponding author: School of Computer Science, Gyeongsang National University, 501, Jinju-daero, Jinju, Gyeongsangnam-do, 52828 Republic of Korea, Tel: +82-55-772-1381

The ciphertext can be decrypted into the same message by both independent receivers using their own private keys. This cryptographic primitive has applications in constructing denial of service attack-resilient protocols, construction of combined cryptosystems, deniable authentication, and to secure the data transfer between various nodes in technologies such as big data analysis, cloud computing, etc., where there is an inherent need to systematically store and optimally analyze vast amounts of information, obtained from/sent to distributed sources, and also to securely cope up with sensitive data meant for ubiquitous and mobile computing applications. In CT-RSA 2014, Chow, Franklin, and Zhang[6] appended the soundness property to the DRE. This new cryptographic primitive has applications in construction of complete non-malleability and plaintext-awareness public key encryption.
In 1994, Shor[7] presented a polynomial time quantum algorithm which can solve discrete logarithm problem (DLP) and prime factorization. This particular algorithm initiated research on Post-Quantum Cryptography (PQC). PQC are the cryptographic algorithms which are secure against classical computers as well as quantum computers. Public key cryptosystems based on code-based cryptography, hash based cryptography, lattice based cryptography and multivariate-quadratic based cryptography are conjectured to be secure against classical computers as well as quantum computers. Among these, Lattice-based cryptography holds a great promise for PQC because of its average case / worst case equivalence property, efficiency and simplicity. Security of most popular algorithm (RSA) is based on the assumption that factoring problem is hard on average case. Ajtai in his seminal paper[8] has shown that security of lattice based cryptosystems is based on the assumption on worst case hardness of lattice problems. This generated a lot of interest on lattice based cryptography. In 2009 Regev[9] introduced the learning with errors (LWE) problem and he won the Godel prize in 2018 for introducing the LWE problem. He has proved that average case LWE problem is as hard as finding the worst-case solution to certain lattice hard problems under a quantum reduction.
In 1984 Shamir[10] presented the idea of identity-based cryptosystem (IBC). In this public key cryptosystem, any arbitrary string $\{0,1\}^*$ which uniquely identifies the user can be public key of the user. For example phone number or email can be public key. This results in reduction of cost of creating public key infrastructure (PKI) and system complexity. Although Shamir designed an identity-based signature (IBS) scheme using RSA hard problem but he was unable to design an identity-based encryption (IBE) scheme and this was a open problem for seventeen years. Solutions to this were proposed independently by Cocks[11] and Boneh - Franklin[12]. Suppose Alice wants to make secure communication with Bob through insecure channel. Alice encrypts the message using Bob's email id as public key and sends the ciphertext to Bob. Bob receives the ciphertext and authenticate himself to third party called Public Key Generator (PKG). The task of PKG is to authenticate the identity of user (Bob), compute the private key with respect to email id (identity) of the user and finally communicate the private key to the user securely. Now user decrypts the ciphertext using this private key. In very large network Public Key Generator, the work required of the PKG is too much. So the concept of Hierarchical IBE (HIBE) was presented in[13, 14, 15] to delegate the PKG's workload to lower-level PKGs. However, only root PKG have their own PPs.

Related Work Shweta Agarwal etc al.[9, 16] presented adaptively secure IBE scheme and selective-ID secure HIBE scheme based on LWE assumption. K. Singh etc al.[3, 17] constructed adaptively secure efficient (H)IBE schemes using LWE hard problem. Independent work by Naccache[1] and Chatterjee - Sarkar[2] presented a variant of Waters's identity based encryption scheme to reduce PPs. They have considered an identity of l-bits as l' chunks where size of each chunk is l/l'. This reduces the PP size from l to l' $n \times m$ matrices. This idea was named as blocking technique[3]. K. Singh etc al.[3, 17] also have reduced PP size using blocking technique. DRE may be considered as a particular case of a broadcast encryption scheme. Adela Georgescu[18] constructed a semantically secure anonymous

broadcast encryption scheme under the ring learning with error assumption. Daode Zhang etc al.[4] constructed lattice-based DRE scheme which is indistinguishable against chosen-ciphertext attacks (IND-CCA). Daode Zhang etc al. also constructed IB-DRE scheme in lattice setting which is secure against stronger security notion i.e. adaptive-ID. We present hierarchical identity based dual encryption (HIB-DRE) scheme under LWE assumption. To the best of our knowledge, this gives the first provably secure HIB-DRE scheme in the lattice based setting. Using blocking technique, we have also reduced the PP size.

Daode Zhang etc al.[4] presented adaptive secure IB-DRE scheme. This scheme[4] contains $l+1$, $n \times m$ matrices as PP, where l denotes the number of the bits in identity. Using blocking technique we have reduced the PP size by around factor β. Because of this the size of prime number q in field Z_q is increased by 2^{β} which results in increase in computation cost. We have shown that compared to Daode Zhang etc al.' scheme the the size of the PP can be decreased approximately by 80% and the time complexity (computation cost) is increased by only 1.40% for a suitably chosen β.

2 Cryptography basics

2.1 Notation

Let us denote R, Z and $[j]$ as set of real numbers, set of integers and the set $\{0,1,\ldots,j\}$. We denote small letters, e.g. x as vectors in column form and capital letters, e.g. X as Matrices. We denote $X \leftarrow \psi_{\beta}(q)_q^{m \times m}$ as matrix X whose elements are chosen from the Gaussian (Normal) distribution ψ_{β} over Z_q and $S \leftarrow Z_q^{n \times m}$ as matrix S whose elements are chosen uniformly over Z_q where Z_q denotes the set $\{0,1,\ldots,q-1\}$. $\langle \mathrm{u,v} \rangle$ represents scalar product of vectors u and v. Symbol $\|.\|$ denotes the standard Euclidean norm in R^n.

Formally, $g(n)$ is negligible function if $g(n) = o(n^{-c})\ \forall$ *constant* c and $n \geq n_0$, where o is standard *little-oh* notation.

Gram Schmidt Orthogonalization (GSO): Let $V = \{v_1,\ldots,v_k\} \subset R^m$ be the set of linearly independent vectors and $\widetilde{V} := \{\widetilde{v_1},\ldots,\widetilde{v_k}\} \subset R^m$ represents the Gram-Schmidt Orthogonalization (GSO) of the $V = \{v_1,\ldots,v_k\} \subset R^m$ which is defined as follows:

$$\widetilde{v_i} = v_i - \sum_{j=1}^{i-1} \Lambda_{i,j}\widetilde{v_j} \ ; \ \Lambda_{i,j} = \frac{\langle v_i, \widetilde{v_j} \rangle}{\langle \widetilde{v_j}, \widetilde{v_j} \rangle}.$$

In other words, $\widetilde{v_1} = v_1$ and $\widetilde{v_2}$ is the component of v_2 orthogonal to the plane which contain vectors v_1, v_2 ($span(v_1, v_2)$). $\widetilde{v_i}$ is orthogonal to span$(v_1,\ldots,v_i)$ where $3 \leq i \leq k$ and component of v_i.[19]

2.2 Hierarchical IB-DRE and IB-DRE

Here definitions of HIB-DRE and IB-DRE are adapted from[13, 14, 15, 16, 4, 20]. User at depth l is represented as sequence of l ids and denoted by : $(id/id_l) = (id_1,\ldots,id_l)$. Ancestors of the user's id tuples are the prefix of (id/id_l). The prefix of (id/id_l) includes lower level PKG and the root PKG. HIB-DRE consists of following four algorithms.

Gen(d,n) This particular algorithm accepts the input as d (the hierarchy tree's greatest depth) and security parameter n and calculates the root PKG's master key and PPs.

Derive$((id/id_l), PP, PR_{(id/id_{l-1})})$ This particular algorithm takes the input as an identity (id/id_l), PP and the private key $PR_{(id/id_{l-1})}$ owned by parent identity $(id/id_{l-1}) = (id_1, \ldots, id_{l-1})$ at depth $l-1 \geq 0$, and computes private key owned by the identity (id/id_l) at depth l.
If $l = 1$ then $PR_{(id/id_0)}$ denotes the root PKG's master key.
For any identity $(id/id_l) = (id_1, \ldots, id_l)$ it is possible to compute the corresponding private key at a depth l by a prefix or an ancestor of the identity (id/id_l) and PKG by repeated calls to the Derive algorithm.

Enc$((id^{1st}/id_l), PP, (id^{2nd}/id_l), M)$ This particular algorithm takes the input as an identity $(id^{1st}/id_l), (id^{2nd}/id_l)$, PP and a message M, and computes ciphertext C.

Dec$(PR_{id^i/id_l}, PP, C)$ This particular algorithm takes the input as one private key $PR_{(id^i/id_l)}$ (where $i \in \{1,2\}$), PPs PP and an encrypted text C, and computes the plain-text message M.

IBE HIBE becomes IBE when depth $l = 1$.

Correctness For all identities (id^{1st}/id_l),(id^{2nd}/id_l), all message M and ciphertext

C=Encrypt(PP,(id^{1st}/id_l),(id^{2nd}/id_l),M) Pr[Decrypt(PP,PR_{id^{1st}/id_l},C)
= Decrypt(PP,PR_{id^{2nd}/id_l},C) = M] = 1 - negl(n)

2.3 Adaptive-ID Security Model of HIB-DRE and IB-DRE

Here definitions of HIB-DRE and IB-DRE are adapted from [13, 14, 15, 16, 4]. Adaptive-ID security model of HIB-DRE is defined using the following game played between an adversary and a challenger. It captures that the challenge ciphertext can not be distinguished from a random element in the ciphertext space. This property implies both recipient anonymity and semantic security.

Gen The challenger runs Gen(λ, d) and keeps master key MK to itself and gives the PP to an adversary.

Phase 1 An adversary can ask private key query for an identity $(id/id_k) = (id_1, \ldots, id_k)$, $k \leq d$. Adversary can also ask private key query for different identities adaptively multiple times.

Challenge The adversary sends message M and identity id^{1*}, id^{2*}. Identity id^{1*}, id^{2*} and the prefix of id^{1*}, id^{2*} is not in phase 1's identity query. Then the challenger randomly picks a bit $r \in \{0,1\}$ and a random C from ciphertext space. If $r = 0$ it assigns the challenge ciphertext i.e. $C^* := Encrypt(PP, id^{1*}, id^{2*}, M)$. If $r = 1$, then the challenge ciphertext is assigned to $C^* := C$. Challenger sends C^* to an adversary.
Phase 2: Again adversary can ask private key query for an identity (id/id_k) as in Phase 1 with the restriction that the adversary is not able to query for id^{1*}, id^{2*} and prefix of id^{1*}, id^{2*}.
Guess: After this adversary makes a guess $r' \in \{0,1\}$ and would win the game if $r = r'$.
The advantage of an IND-ID-CPA adversary A in attacking the IB-DRE scheme ξ is defined as We claim that HIB-DRE scheme ξ with depth d is adaptive-ID, indistinguishable from being random if for all IND-ID-CPA PPT adversaries A, $Adv_{d,\xi,A}(\lambda)$ is negligible.

IBE Security model of HIB-DRE becomes security model of IB-DRE when the hierarchy tree is of depth one.

2.4 Integer Lattices ([21])

An Integer lattice is defined to be the set of all integer combinations

$$L(v_1,\ldots,v_n) = \{x_1v_1 + \cdots + x_nv_n : x_1,\ldots,x_n \in Z\}$$

of n linearly independent vectors $\{v_1,\ldots,v_n\} \in R^n$. The set of vectors $\{v_1,\ldots,v_n\}$ is called a basis for the lattice. A basis can be represented by the matrix $B = [v_1,\ldots,v_n] \in R^{n\times n}$ with the columns containing the basis vectors. In matrix notation, the lattice generated by $n \times n$ matrix $B \in R^{n\times n}$ can be defined as $L(V) = \{Vx : x \in Z^n\}$, where Vx is the multiplication of $n \times n$ matrix and $n \times 1$ vector. The determinant of a lattice is the absolute value of the determinant of the basis matrix $det(L(V)) = |det(V)|$. For prime q, matrix $M \in Z_q^{n\times m}$ and vector $v \in Z_q^n$, define:

$$\Lambda_q(M) := \{t \in Z_q^m \ \ s.t.\ \ \exists s \in Z_q^n \text{ where } M^T s = t \ (mod\ q)\}$$

$$\Lambda_q^{\perp}(M) := \{t \in Z_q^m \ \ s.t.\ \ Mt = 0 \ (mod\ q)\}$$

$$\Lambda_q^{u}(M) := \{t \in Z_q^m \ \ s.t.\ \ Mt = v \ (mod\ q)\}$$

Theorem 2.1. *([8, 22]) Let q be odd prime and $m := \lceil 6n\lg q \rceil$. Then there is a probabilistic polynomial-time (PPT) algorithm TrapGen(q,n) that computes a pair ($A \in Z_q^{n\times m}, T \in Z^{m\times m}$) s. t. A is statistically close to a uniform matrix in $Z_q^{n\times m}$ and vector T is a basis for $\Lambda_q^{\perp}(A)$ satisfying*

$$\|T\| \le O(n\lg q)\ ,\ \ \|\widetilde{T}\| \le O(\sqrt{n\lg q})$$

Lemma 1 [22]. Let q be odd prime and M be a matrix in $Z_q^{n\times m}$ with $m > n$. Let T_M be a basis for $\Lambda_q^{\perp}(M)$ and
$\sigma \ge \|\widetilde{T_M}\|\omega(\sqrt{(\lg m)})$. Then for $c \in R^m$ and $u \in Z_q^n$:

1. There exists a PPT algorithm SampleGaussian (M, T_M, σ, c) that returns $x \in \Lambda_q^{\perp}(M)$ drawn from a distribution statistically close to $D_{\Lambda,\sigma,c}$.
2. There exists a PPT algorithm SamplePre (M, T_M, u, σ) that returns $x \in \Lambda_q^{u}(M)$ sampled from a distribution statistically close to $D_{\Lambda_q^u,\sigma}$.

Lemma 2[22]. Suppose that $m > (n+1)\_2q + w(\lg n)$ and that q is prime. Let A,B be matrices chosen uniformly in $Z_q^{n\times m}$ and let $R \in \{1,-1\}^{m\times m}$ be an uniform random matrix. Then, for all vectors $w \in Z_q^m$, the distribution (A,B,R^Tw) and (A,AR,R^Tw) are close (statistically) to each other.

2.5 The Learning With Errors (LWE) Hardness Assumption

In 2009 Oded Regev[9] introduced the LWE problem and he won the Godel prize in 2018 for introducing the LWE problem. He proved that under a quantum reduction LWE too has a similar equivalence hardness property in the average case / worst case. LWE problem has two versions: Search and decision.

Search Consider an odd prime q, a positive integer n, and a Gaussian (Normal) distribution χ^m over Z_q^m.
Given $(A, As+e)$ where matrix $A \in Z_q^{m\times n}$ is uniformly random and $e \in \chi^m$, finding s is hard.

Decision[9, 16] Consider a odd prime q, a positive integer n, and a Gaussian (Normal) distribution χ^m over Z_q^m. The pair (A, v) is the input from an unspecified challenge oracle O, where $m \times n$ matrix $A \in Z_q^{m \times n}$ is uniformly chosen. An unspecified challenge oracle O is either a noisy pseudo-random sampler O_s or a truly random sampler $O_\$$. It depends on how v is selected.

1. When v is computed as $As + e$ for a vector $e \in \chi^m$ and a randomly chosen $s \in Z_q^n$. Then O, an unspecified challenge oracle, is a noisy pseudo-random sampler O_s.

2. When v is chosen uniformly from Z_q^m, an unspecified challenge oracle O is a truly random sampler $O_\$$.

The adversary would try to tell the above two cases apart with a significant probability.
Or it could be said that A, an algorithm, decides the (Z_q, n, χ)-*LWE* problem if $|Pr[A^{O_s} = 1] - Pr[A^{O_\$} = 1]|$ = non-negligible for a random chosen $s \in Z_q^n$.
It is also proved in[23, 24] that above decision LWE too is a hard problem even in the case where s is chosen from the Gaussian (Normal) distribution.

2.6 SIS Assumption[8]

In 1996 Ajtai[8] presented Small Integer Solution (SIS) and Inhomogeneous Small Integer Solution (ISIS) hard problems.

Definition 6 For an integer q, a matrix $A \in Z_q^{n \times m}$ and a real β, find a *short (nearly orthogonal)* m-dimensional vector $x \in Z_q^m$ which satisfies the equations $Ax = 0 \ mod \ q$ and $\|x\| \leq \beta$. OR
find a vector $x \in Z_2^m$ which satisfies the equation $Ax = 0 \ mod \ q$.

2.7 ISIS Assumption

Definition 7 Given a matrix $A \in Z_q^{n \times m}$, an integer q, a n-dimensional vector $u \in Z_q^n$ and real β, find a *short (nearly orthogonal)* m-dimensional vector $x \in Z_q^m$ which satisfies the equations $Ax = u \ mod \ q$ and $\|x\| \leq \beta$. OR
find a m-dimensional vector $x \in Z_2^m$ which satisfies the equation $Ax = u \ mod \ q$.

3 Algorithms

Let $M \in Z_q^{n \times m}$, $M_1 \in Z_q^{n \times m_1}$ and $F = MM_1 \in Z_q^{n \times (m+m_1)}$ be matrices. We will need to sample short vector and short (nearly orthogonal) basis in $\Lambda_q^u(F)$ for some u in Z_q^n using either a SampleLeft or SampleBasisLeft algorithm.

3.1 SampleLeft Algorithm [16]

SampleLeft Algorithm(M_1, M, T_M, u, σ): This particular algorithm accepts argument a matrix M_1 in $Z_q^{n \times n_1}$, a rank n matrix M in $Z_q^{n \times m}$, a "short (nearly orthogonal) " basis T_M of $\Lambda_q^\perp(M)$, a vector $u \in Z_q^n$ and a Gaussian (Normal) parameter $\sigma > \|\widetilde{T_M}\| \omega(\sqrt{(\lg(m+n_1))})$. This particular algorithm computes a vector $e \in Z^{m+n_1}$ sampled from a distribution close (statistically) to $D_{\Lambda_q^u(F_1),\sigma}$, where $F_1 = M|M_1$.

3.2 SampleBasisLeft Algorithm[16]

SampleBasisLeft Algorithm(M_1, M, T_M, u, σ): This particular algorithm accepts argument a matrix M_1 in $Z_q^{n\times n_1}$, a rank n matrix M in $Z_q^{n\times m}$, a "short (nearly orthogonal) " basis T_M of $\Lambda_q^{\perp}(M)$, a vector $u \in Z_q^n$ and a Gaussian (Normal) parameter $\sigma > \|\widetilde{T_M}\|\omega(\sqrt{(\lg(m+n_1))})$. Finally this particular algorithm computes a short basis S of $\Lambda_q^{\perp}(F)$ where $F_1 = M|M_1$.
Let $A, D \in Z_q^{n\times m}$, $R \in \{-1,1\}^{m\times m}$ and $F = (AR+D) \in Z_q^{n\times 2m}$ be matrices. We will need to sample short (nearly orthogonal) vector and short (nearly orthogonal) basis in $\Lambda_q^u(F)$ for some u in Z_q^n using either a SampleRight or SampleBasisRight algorithm. Let $s_R := \|R\|$, and a Gaussian(Normal) parameter $\sigma > \|\widetilde{T_D}\| s_R \omega(\sqrt{\lg(m)})$.

3.3 SampleRight Algorithm[16]

SampleRight Algorithm$(A, D, T_D, R, \sigma,$ **u**$)$: This particular algorithm takes as input a matrix A of rank n in $Z_q^{n\times m}$, D in $Z_q^{n\times m}$ (where D is rank n), a basis T_D of $\Lambda_q^{\perp}(D)$, a vector $u \in Z_q^n$, a matrix R in $Z_q^{k\times m}$, and computes a (m+k)-dimensional vector $e \in Z^{m+k}$ sampled from a distribution statistically close to $D_{\Lambda_q^u(F_2),\sigma}$ where $F_2 = (A|AR+D)$.

3.4 SampleBasisRight Algorithm[16]

SampleBasisRight Algorithm$(A, D, T_D, R, u, \sigma)$: This particular algorithm accepts as argument a rank n matrix A in $Z_q^{n\times m}$, D in $Z_q^{n\times m}$ of rank n, a basis T_D of $\Lambda_q^{\perp}(D)$, a m+k-dimensional vector $u \in Z_q^n$, a matrix R in $Z_q^{k\times m}$ and computes a short (nearly orthogonal) basis S of $\Lambda_q^{\perp}(F_2)$ where $F_2 = (A|AR+D)$,

4 Hierarchical Identity based Dual Receiver Encryption (HIB-DRE) scheme

We present Hierarchical Identity based Dual Receiver Encryption (HIB-DRE) scheme in stronger security notion i.e. adaptive-ID with short (nearly orthogonal) PPs. Our construction is a variant of schemes[16, 3, 17]. In our construction, identity id/id_l is denoted as $id/id_l = (id_1, \ldots, id_l) = ((b_{1,1}||\ldots||b_{1,l''}), \ldots, (b_{l,1}||\ldots$ where id_i is l' bit string and $b_{i,j}$ is $\beta(= l'/l'')$ bit string. Encryption matrix for selective-ID secure lattice based HIBE scheme in[16] is defined as

$$E_{id} = (A_0|A_1 + H(id_1)D|\ldots|A_l + H(id_l)D) \in Z_q^{n\times(l+1)m}$$

We use Brent R. Waters's method[25] to convert Agrawal etc al. selective-ID secure lattice HIB-DRE[16] to adaptive-ID secure HIB-DRE. With this method, PPs for an l-level HIB-DRE are $A_{1,1}, \ldots, A_{1,l'}, A_{2,1}, \ldots, A_{2,l'}, \ldots, A_{l,1'}, \ldots$ $A'_{1,1}, \ldots, A'_{1,l'}, A'_{2,1}, \ldots, A'_{2,l'}, \ldots, A'_{l,1}, \ldots, A'_{l,l'}$, and A_0, D matrices. Now encryption matrix for first identity (id^1) becomes

$$F_{id^1/id_l} = \left(A_0|\sum_{j=1}^{l'} A_{1,j}b_{1,j} + D|\ldots|\sum_{j=1}^{l'} A_{l,j}b_{l,j} + D\right)$$

and for encryption matrix for second identity (id^2) becomes

$$F_{id^2/id_l} = \left(A'_0|\sum_{j=1}^{l'} A'_{1,j}b_{1,j} + D|\ldots|\sum_{j=1}^{l'} A'_{l,j}b_{l,j} + D\right)$$

The PPs is $2l \times l' + 2$ matrices which is very large. We have used same PPs $A_1, \ldots, A_l$ for all levels as done in[26]. This way we have reduced PPs from $2l \times l' + 2$ matrices to $2l' + 2$ matrices. Further using

the blocking technique of Chatterjee - Sarkar's[2], we have reduced the PPs from $(2l'+2)$ matrices to $(2l''+2)$ matrices. Finally our scheme has two encryption matrices. Encryptiom matrix for first identity is defined as:

$$F_{id^1/id_l} = \left(\sum_{j=1}^{l''} A_j b_{1,j} + D | \sum_{j=1}^{l''} A_j b_{2,j} + D | \ldots | \sum_{j=1}^{l''} A_j b_{l,j} + D \right) \tag{1}$$

where $id^1/id_l = (id_1, \ldots, id_l) = ((b_{1,1}||\ldots||b_{1,l''}), \ldots,$
$(b_{l,1}||\ldots||b_{l,l''}))$, id_i is l' bit string and $b_{i,j}$ is $l'/l'' = \beta$ bit string.
Encryptiom matrix for second identity is defined as:

$$F_{id^2/id_l} = \left(\sum_{j=1}^{l''} A_j b'_{1,j} + D | \sum_{j=1}^{l''} A_j b'_{2,j} + D | \ldots | \sum_{j=1}^{l''} A_j b'_{l,j} + D \right) \tag{2}$$

where $id^2/id_l = (id_1, \ldots, id_l) = ((b'_{1,1}||\ldots||b'_{1,l''}), \ldots,$
$(b'_{l,1}||\ldots||b'_{l,l''}))$, and id_i, $b'_{i,j}$ are l', $l'/l''(=\beta)$ bit strings respectively.

4.1 The HIB-DRE Scheme

Our adaptive secure HIB-DRE scheme is described as follows.

Gen(d,n) Input to this particular algorithm are maximum hierarchy depth d and security parameter n. This particular algorithm computes the PPs and master secret key. Algorithm executes following steps.

1. TrapGen(q,n) algorithm is used to generate a pair of matrices $A_0, A'_0 \in Z_q^{n\times m}$ and a pair of short (nearly orthogonal) basis $T_{A_0}, T_{A'_0}$ for $\Lambda_q^{\perp}(A_0)$ and $\Lambda_q^{\perp}(A'_0)$ such that $\|\widetilde{T_{A_0}}\| \leq O(\sqrt{n \lg q})$ and $\|\widetilde{T_{A'_0}}\| \leq O(\sqrt{n \lg q})$.

2. Select $2l''+1$ matrices

$$A_1, A_2, \ldots, A_{l''}, A'_1, A'_2, \ldots, A'_{l''} \text{ and } D \in Z_q^{n\times m}$$

randomly.

3. Select a matrix $U \in Z_q^{n\times n}$ randomly.

4. PPs PP = $A_1, A_2, \ldots, A_{l''}, A'_1, A'_2, \ldots, A'_{l''}, D,$ and $A_0 \in Z_q^{n\times m}$, $U \in Z_q^{n\times n}$,
Master key (MK) = $T_{A_0} \in Z_q^{m\times m}$.

Derive$(PP, (id/id_l), PR_{(id/id_{(l-1)})})$ Input to this particular algorithm are PPs (PP), identity (id/id_l) and private key $\text{PR}_{(id/id_{l-1})}$ owned by an identity (id/id_{l-1}) at depth $l-1$. It computes a short (nearly orthogonal) basis and private key for the identity (id/id_l) at depth l. Here encryption matrix F_{id/id_l} for the id/id_l is:

$$F_{id/id_l} = \left(A_0 | \sum_{j=1}^{l''} A_j b_{1,j} + D | \ldots | \sum_{j=1}^{l''} A_j b_{l,j} + D \right)$$

$$F_{id/id_l} = \left(F_{id/id_{l-1}} | \sum_{j=1}^{l''} A_j b_{l,j} + D \right). \tag{4}$$

With short (nearly orthogonal) basis $PR_{(id/id_{(l-1)})}$ for $\Lambda_q^{\perp}(F_{id/id_{l-1}})$ and encryption matrix F_{id/id_l} as defined in (3), we can compute short (nearly orthogonal) basis $PR_{(id/id_l)}$ for $\Lambda_q^{\perp}(F_{id/id_l})$ by invoking SampleBasisLeft (SBL) algorithm

$$S \leftarrow \text{SBL}(F_{id/id_{l-1}}, \sum_{j=1}^{l''} A_j b_{l,j} + D, PR_{(id/id_{(l-1)})}, 0, \sigma_l)$$

and compute $PR_{(id/id_l)} \longleftarrow S$.
With short (nearly orthogonal) basis $PR_{(id/id_{(l-1)})}$ for $\Lambda_q^{\perp}(F_{id/id_{l-1}})$ and encrypted matrix F_{id/id_l} as defined in (3), we can compute private key $e_{(id/id_l)}$ for $\Lambda_q^{\perp}(F_{id/id_l})$ by invoking

$$S \longleftarrow \text{SampleLeft}(F_{id/id_{l-1}}, \sum_{j=1}^{l''} A_j b_{l,j} + D, PR_{(id/id_{(l-1)})}, 0, \sigma_l)$$

and compute $e_{(id/id_l)} \longleftarrow S$.
For an identity $(id/id_l) = (id_1, \ldots, id_l)$, the corresponding private key at a depth of l can be calculated by PKG or any prefix or ancestor of an identity (id/id_l) by repeated calls to the SampleBasisLeft algorithm and finally calling SampleLeft algorithm.

Enc(PP, Id, m) Input to this particular algorithm are PPs PP, identities $(id^1/id_l), (id^2/id_l)$ of depth l and a message $m \in \{0,1\}^n$. Next algorithm executes following steps:

1. Encryption matrix for id^1 and id^2 as defined in equation (1) and (2) are:
   $F_{id^1/id_l} =$
   $$\left(A_0 | \sum_{j=1}^{l''} A_j b_{2,j} + D | \sum_{j=1}^{l''} A_j b_{2,j} + D | \ldots | \sum_{j=1}^{l''} A_j b_{l,j} + D\right) \in Z_q^n \times Z_q^{(l''+1)m}$$
   $F_{id^2/id_l} =$
   $$\left(A_0' | \sum_{j=1}^{l''} A_j b_{1,j} + D | \sum_{j=1}^{l''} A_j b_{2,j} + D | \ldots | \sum_{j=1}^{l''} A_j b_{l,j} + D\right) \in Z_q^n \times Z_q^{(l''+1)m}$$

2. Choose a n-dimensional random vector $s \xleftarrow{R} Z_q^n$ uniformly.

3. Choose l'' random $m \times m$ matrices $R_j \xleftarrow{R} \{-1,1\}^{m \times m}$ for $j = 1, \ldots, l''$ uniformly.
   Define $R_{id}{}^1 = \sum_{j=1}^{l''} b_j R_j || \ldots || \sum_{j=1}^{l''} b_j R_j \in Z^{m \times l''m}$.

4. Choose a n-dimensional random vector $s \xleftarrow{R} Z_q^n$ uniformly.

5. Choose l'' random $m \times m$ matrices $R_j \xleftarrow{R} \{-1,1\}^{m \times m}$ for $j = 1, \ldots, l''$ uniformly.
   Define $R_{id}{}^2 = \sum_{j=1}^{l''} b_j R_j || \ldots || \sum_{j=1}^{l''} b_j R_j \in Z^{m \times l''m}$.

[1]In security proof, R_{id} would be used to reply attacker's private key query. Error vector has to be $\begin{bmatrix} y \\ R_{id}^T y \end{bmatrix}$ for valid challenge ciphertext

[2]In security proof, R_{id} would be used to reply attacker's private key query. Error vector has to be $\begin{bmatrix} y \\ R_{id}^T y \end{bmatrix}$ for valid challenge ciphertext

6. Choose a n-dimensional noise vector $x \xleftarrow{\overline{\Psi}_{\alpha_l}} Z_q^n$, $y \xleftarrow{\overline{\Psi}_{\alpha_l}^m} Z_q^m$, $y_1 \xleftarrow{\overline{\Psi}_{\alpha_l}^m} Z_q^m$ and $z \longleftarrow R_{id}^T y \in Z_q^{l''m}$, $z_1 \longleftarrow R_{id}^T y_1 \in Z_q^{l''m}$

7. Finally the ciphertext is:

$$CT = (C_0 = U^T s + x + b\lfloor \frac{q}{2} \rfloor, C_1 = F_{id^1/id_l}^T s + \begin{bmatrix} y \\ z \end{bmatrix},$$

$$C_2 = F_{id^2/id_l}^T s + \begin{bmatrix} y_1 \\ z_1 \end{bmatrix} \in Z_q^n \times Z_q^{(l''+1)m} \times Z_q^{(l''+1)m})$$

Dec$(PP, \mathbf{PR}_{(id^i/id_l)}, CT)$ Input to this particular algorithm are PPs PP, a private key of the i^{th} identity PR_{id^i/id_l} $i \in \{1,2\}$, and a ciphertext CT = (C_0, C_1, C_2). Next algorithm executes following steps:.

1. Set $\tau_l = \sigma_l \sqrt{m(l+1)} w(\sqrt{lg(lm)})$.
   Then $\tau_l \geq \|\widetilde{PR}\| w(\sqrt{lg(lm)})$.

2. $e_{id^i/id_l} \longleftarrow SamplePre(F_{id^i/id_l}, PR_{(Id^i/id_l)}, U, \tau_l)$
   Then $F_{id^i/id_l} e_{id^i/id_l} = U$ and $\|e_{id^i/id_l}\| \leq \tau_l \sqrt{m(l+1)}$

3. For identity i, compute $w = w_1 w_2 \ldots w_n = C_0 - e_{id^i/id_l}^T C_i \quad \in Z_q^n$.

4. For j = 1 to n
   if $|w_i - \lfloor \frac{q}{2} \rfloor| < \frac{q}{4}$ in Z, $w_i = 1$ else $w_i = 0$.

During Decryption:
$w = C_0 - e_{id^i/id_l}^T C_i = b\lfloor \frac{q}{2} \rfloor + x - e_{id^i/id_l}^T \begin{bmatrix} y \\ z \end{bmatrix}$.

Correctness After decryption, error term
$e = e_1 e_2 \ldots e_n = x - e_{id^i/id_l}^T \begin{bmatrix} y \\ z \end{bmatrix}$. And for correctness of HIB-DRE scheme $e_i < q/4$ for all i.

Lemma 3 Norm of the error term is bounded by $[q 2^\beta l'' l^2 \sigma_l m \alpha_l \omega(\sqrt{\lg m})$
$+ O(2^\beta l'' l^2 \sigma_l m^{3/2})]$. **Proof**: This Lemma is very similar to lemma 32 of [16] except now R_{id} is uniformly random $m \times lm$ matrix in $\{-2^\beta l'', 2^\beta l''\}^{m \times lm}$. So $|R_{id}|$ will be equal to $2^\beta l'' R_{id}$. So error term will have extra factor $2^\beta l''$.

Now, for correctness of the scheme we have to make sure that:

- the error $< q/5$ i.e. $\alpha_l < [2^\beta l'' l^2 \sigma_l m \omega(\sqrt{\lg m})]^{-1}$ and $q = \Omega(2^\beta l'' l^2 \sigma_l m^{3/2})$
- $m > 6n \lg q$ to execute TrapGen algorithm.
- That σ_l is sufficiently large enough for the algorithm SampleLeft and algorithm SampleRight (i.e. $\sigma_l > \|\widetilde{T_D}\| s_R \omega(\sqrt{\lg m})$) $= 2^\beta l'' \sqrt{l} m \omega(\sqrt{\lg m})$
- that Regev's reduction applies (i.e. $(q 2^\beta)^l > 2Q$), where Q is the number of times the adversary queries the identity.

To meet the above requirements we have to assign the parameters $(q, m, \sigma_l, \alpha_l)$ with respect to security parameter n as follows:

$$\alpha_l = [(2^\beta l'')^2 l^{2.5} m^2 \omega(\sqrt{\lg m})]^{-1} \tag{5}$$
$$q = max((2Q/2^\beta)^{1/l}, (2^\beta l'')^2 l^{2.5} m^{2.5} \omega(\sqrt{\lg n})),$$
$$\sigma_l = l''\sqrt{l} m \omega(\sqrt{\lg n}), \qquad m = 6n^{1+\delta}$$

From above requirements, we need $q = (2^\beta l'')^2 l^{2.5} m^{2.5} \omega(\sqrt{\lg n})$.

4.2 Security Proof

Security proof is based on the game played between an adversary and challenger. In this process adversary can ask private key query for polynomial number of identities to the challenger. If the challenger fails to answer the private key query the game will be aborted. In our proof, game will not be aborted if challenger can not answer the private key query for challenged identities id^{1*}, id^{2*} and will be able to answer private key query for other identities. Abort-resistant hash functions is used to compute no abort probabilities. It is defined as follows.

4.2.1 Abort-Resistant Hash Functions

Definition 5 Suppose function $H = \{\hbar : X \longrightarrow Y\}$ be family of hash functions from X to Y. For a set of $Q+2$ inputs $\bar{x} = (x_0^1, x_0^2, x_1, \ldots, x_Q) \in X^{Q+2}$, non-abort probability of $\bar{x}$ i.e. $\alpha(\bar{x})$ is as

$$\alpha(\bar{x}) = Pr\left[\hbar[x_0^1] = 0 \ \wedge \ \hbar[x_0^2] = 0 \ \wedge \ \hbar[x_1] \neq 0 \ \wedge \ldots \wedge \hbar[x_Q] \neq 0\right]$$

Here the probability is computed based on the random choice of $\hbar$ in H.
We say that H is $(Q, \alpha_{min}, \alpha_{max})$ abort-resistance if for all $\bar{x} = (x_0^1, x_0^2, x_1, \ldots, x_Q) \in X^{Q+2}$ with $x_0^1, x_0^2 \notin \{x_1, \ldots, x_Q\}$ we have $\alpha(\bar{x}) \in [\alpha_{min}, \alpha_{max}]$.
Following abort-resistant hash family is used which is very similar to [16].
For a q (prime) let $(Z_q^{l''})^* = Z_q^{l''}$-$\{0^{l''}\}$ and define the family

$$H : \{\hbar : ((Z_{2^\beta}^{l''})^* | \ldots | (Z_{2^\beta}^{l''})^*) \longrightarrow (Z_q | \ldots | Z_q)\}$$

$$\hbar(id) = \hbar(id_1 | \ldots | id_l) = \left(1 + \sum_{j=1}^{l''} h_j b_{1,j}\right) | \ldots | \left(1 + \sum_{j=1}^{l''} h_j b_{l,j}\right) \tag{6}$$

For definition of h_i and $b_{k,i}$ see section 4.2.2.

4.2.2 Lemma 4

let q be a odd prime and $0 < Q < q$. Then the hash family H defined in (5) is $(Q, \frac{1}{q^{2l}}(1 - \frac{Q}{q^l}), \frac{1}{q^{2l}})$ abort-resistant.

4.2.3 Proof

The proof for this is similar to[16]. Consider a set of $\overline{id}$ of $Q+1$ inputs $id^0,\ldots,id^Q$ in $(Z_q^{ll''})^*$ where $id^0 \notin \{id^1,\ldots,id^Q\}$ and $id^i = \{id_1,\ldots,id_l\}$. Since number of functions in $H = q^{l''}(2^\beta)^{l''l}$ and for $i = 0,\ldots,Q+1$ let S_i be the set of functions $\hbar$ in H such that $\hbar(id^i) = 0$. So number of these functions $= |S_i| = \frac{q^{l''}(2^\beta)^{l''l}}{q^l}$.
And $\frac{|S_0 \wedge S_j| \leq q^{l''}(2^\beta)^{l''l}}{q^{2l}}$ for every $j > 0$. Number of functions in H such that $\hbar(id^0) = (0|\ldots|0)$ but $\hbar(id^i) \neq 0$ for $i = 1,\ldots,Q$. $= |S|$ and

$$|S| = |S_0^1 \wedge S_0^2 - (S_1 \wedge \ldots S_Q)| \geq |S_0^1 \wedge S_0^2| - \sum_{j=1}^{Q} |S_0^1 \wedge S_0^2 \wedge S_j|$$

$$\geq \frac{q^{l''}(2^\beta)^{l''l}}{q^{2l}} - Q\frac{q^{l''}(2^\beta)^{l''l}}{q^{3l}}$$

Hence identities' no-abort probability is at least equal to $\frac{\frac{q^{l''}(2^\beta)^{l''l}}{q^l} - \frac{Qq^{l''}(2^\beta)^{l''l}}{q^{2l}}}{q^{l''}(2^\beta)^{l''l}} = \frac{1}{q^{2l}}(1-\frac{Q}{q^l})$
Since $|S| \leq |S_0|$, hence the no-abort probability is $\leq \frac{|S_0|}{q^{l''}(2^\beta)^{l''l}} = \frac{1}{q^{2l}}$.

Now we show that under a adaptive identity attack our scheme is indistinguishable from random. It is IND-ID-CPA secure.

Theorem 4.1. *If $(Z_q, n, \bar{\Psi}_{\alpha_d})$-LWE assumptions holds then our Full HIB-DRE scheme is IND-ID-CPA secure.*

Proof The proof of this is similar to[16, 3]. We will show that if there exists a Probabilistic Polynomial-Time (PPT) adversary $\mathscr{A}$ that breaks our $HIB-DRE$ scheme in polynomial time with a significant probability, then there exists a Probabilistic Polynomial-Time challenger $\mathscr{B}$ that would answer if an oracle O (unspecified challenge) is truly either a random sampler $O_\$$ or a noisy pseudo-random sampler O_s by simulating views of adversary $\mathscr{A}$ (solves LWE problem) .

Setup Challenger $\mathscr{B}$ randomly choose $n \times m$ matrix $A_0 \in Z_q^{n\times m}$. Using algorithm TrapGen algorithm, matrix $D \in Z_q^{n\times m}$ and a Trapdoor T_D for $\Lambda_q^\perp(D)$ is generated. Challenger also chooses l'' uniformly random matrices $R_i \in [-1,l]^{m\times m}, i \in [1,l'']$ and l'' random scalars $h_i \in Z_q, i \in [1,l'']$. Next it constructs the matrices A_i as

$$A_i \longleftarrow A_0 R_i + h_i D \tag{7}$$

By lemma 2, the distribution of A_i's are statistically close to the uniform distribution.

$$F_{id/id_l} = \left(A_0|\sum_{j=1}^{l''} A_j b_{1,j} + D||\ldots||\sum_{j=1}^{l''} A_j b_{l,j} + D\right)$$

Substituting the value of matrices A_i from equation (6)

$$F_{id/id_l} = \left(A_0|A_0\left(\sum_{j=1}^{l''} R_j b_{1,j}\right) + D\left(1+\sum_{j=1}^{l''} h_j b_{1,j}\right)||\ldots||\right)$$

$$A_0\left(\sum_{j=1}^{l''} R_j b_{l,j}\right) + D\left(1 + \sum_{j=1}^{l''} h_j b_{l,j}\right)$$

Or
$F_{id} = (A_0' | A_0 R_{id} + D h_{id})$
where $R_{id} = \sum_{j=1}^{l''} R_j b_{1,j} || \ldots || \sum_{j=1}^{l''} R_j b_{l,j}$
and $D_{id} = D\hbar_{id} = D(1 + \sum_{j=1}^{l''} h_j b_{1,j}) || \ldots || D(1 + \sum_{j=1}^{l''} h_j b_{l,j})$
If $\hbar_{id}$ is equal to zero then challenger will not be able to answer the private key query and it will be part of abort resistant hash function.
Else if $\hbar_{id} \neq 0$ then challenger $\mathscr{B}$ answers the secret key query of $id = (id^1, id^2, \ldots, id^l)$ by running

$$PR_{id} \longleftarrow \text{SampleRight}(A_0, D_{id}, R_{id}, T_D, 0, \sigma_l)$$

and sending PR_{id} to A.

Challenge Adversary declares target identities $id_1^* = (id_1, id_2, \ldots, id_l)$ and $id_2^* = (id_1', id_2', \ldots, id_l')$. Challenger B gets 3 LWE samples i.e. $(U_i, u_i) \in Z_q^{n \times n} \times Z_q^n$ $(0 \leq i \leq 2$ from an oracle.

1. Blind the message $m \in \{0,1\}^n$ by letting

$$C_0^* = u_0 + m^* \lfloor \frac{q}{2} \rceil \in Z_q^n$$

2. Challenger chooses l'' random matrices $R_i^* \in [-1,1]^{m \times m}$ where $i \in [1, l'']$. Let

$$R_{id^*} = (R_1^* | \ldots | R_{l''}^*)$$

and set

$$C_1^* = \begin{pmatrix} u_1^* \\ (R_{id^*})^T v_1^* \end{pmatrix} \in Z_q^{m+l''m}$$

and

$$C_2^* = \begin{pmatrix} u_2^* \\ (R_{id^*})^T v_2^* \end{pmatrix} \in Z_q^{m+l''m}$$

3. Choose a random bit $r \leftarrow \{0,1\}$. If $r = 0$, send $CT^* = (C_0^*, C_1^*, C_2^*)$ to the adversary. If $r = 1$ choose a random $(C_0, C_1, C_2) \in Z_q^n \times Z_q^{m+l''m} \times Z_q^{m+l''m}$ and send (C_0, C_1, C_2) to the adversary.

Phase 2 Except id^* and prefix of id^*, adversary can make secret key query for any id. Simulator repeats the same method used in Setup() part to answer the query.

Artificial Abort In Eurocrypt 2004, Brent R. Waters[25] presented the artificial abort technique. Chatterjee-Sarkar[2] explained artificial abort (AB) steps in detail. Since simulator's abort probability depends on private key queries asked by adversary. So it may be possible that simulator' abort probability and an adversary's success probability are dependent. Objective of the AB technique is to make simulator's abort probability almost same for any set of queries asked by an adversary. AB technique increases the time complexity of the simulation.
Let λ be the probability that simulator does not abort i.e. (1−simulator's abort probability). Suppose *abort* be the event that simulator B aborts, and that Σ' is the set of queries asked by an adversary.

Waters[25] has proved that probability simulator B does not abort is almost λ for all set of queries asked by the adversary.

$$|Pr[\overline{abort}|Y \in \Sigma'] - \lambda| \leq \frac{\lambda\varepsilon}{2}$$

No-abort probability of identities is $\geq \frac{1}{q^l}(1-\frac{Q}{q^{2l}})$ (lemma 4). With $Q \leq q^l/2$ non-abort probability of identities will be $\geq \frac{1}{q^l}$.
for AB steps, simulator requires an additional $\chi = O(\varepsilon^{-2}ln(\varepsilon^{-1})\lambda ln(\lambda^{-1}))$ time . Bellare-Ristenport [27] showed that AB steps can be avoided. Bellare-Ristenport derived following security reduction formula without AB steps.

$$Adv^{dbdh}(B) \geq \frac{\gamma_{min}}{2}Adv^{IND-CPA}_{Waters} + (\gamma_{min} - \gamma_{max})$$

From above expression it is clear that Bellare-Ristenport's [27] proof will work when $\gamma_{min} - \gamma_{max}$ is negligible. But in our case $\gamma_{min} - \gamma_{max}$ is $-\frac{Q}{q^2}$ and it can be made negligible with very large q. large q will increase the computation time of the scheme. So we have used Waters[25] AB.
Since, for non-abort probability $h_{id^*} = 0$ then $F_{id^*} = (A_0|A_0\overline{R}_{id^*})$. When the LWE oracle is pseudorandom

$$v^* = A_0^T s + y$$

for some random noise $y \in Z_q^m$ distributed as $\bar{\psi}_\alpha^m$. Therefore

$$C_1^* = \begin{pmatrix} A_0^T s + y \\ (A_0 R_{id^*})^T s + (R_{id^*})^T y \end{pmatrix} = (F_{id^*})^T s + \begin{pmatrix} y \\ (R_{id^*})^T y \end{pmatrix}$$

Above C_1^* is a valid C_1 part of challenge ciphertext. Again $C_0^* = u_0^T + m^* \lfloor \frac{q}{2} \rceil$ is also a valid C_0 part of challenge ciphertext. Therefore (C_0^*, C_1^*, C_2^*) is valid challenge ciphertext.
When LWE oracle is random oracle, v_0 is uniform in Z_q^n and v^* is uniform in Z_q^m. Therefore challenge ciphertext is always uniform in $\in Z_q^n \times Z_q^{m+l''m} \times Z_q^{m+l''m}$. Finally if adversary $\mathscr{A}$ terminates with correct result then challenger $\mathscr{B}$ answer that an oracle O (unspecified challenge) is a noisy pseudo-random sampler O_s else challenger $\mathscr{B}$ answers that an unspecified challenge oracle O is a truly random sampler $O_\$$ and ends the simulation.
So PPT algorithm B that solves the $(Z_q, n, \overline{\Psi}_\alpha)$-LWE problem with $\varepsilon' \geq \varepsilon/4q^{2l}$ in about the time $= t_1 + O(\varepsilon^{-2}ln(\varepsilon^{-1})\lambda ln(\lambda^{-1}))$. Since no one can solve LWE hard problem so our scheme is also semantically secure.

5 New Full IB-DRE Scheme

Our construction is a variant of Daode Zhang et al. IB-DRE scheme[4], but with shorter PP. In Daode Zhang et al.[4] IB-DRE scheme identity string have l-bits. Therefore, scheme requires l $n \times m$ matrices. We apply the blocking technique of Chatterjee-Sarkar[26] to divide l-bit identity into l' chunks where size of each chunk is $l/l' = \beta$ bits and assign one $n \times m$ matrix to each block. This way we have reduced PPs from l $n \times m$ matrices to l' $n \times m$ matrices.

5.1 The New Full IB-DRE Construction

We present our new Full IB-DRE Scheme.

5.1.1 Setup(n)

This particular algorithm accepts argument as security parameter n computes the PPs and master secret key. Then algorithm executes following steps:

1. Apply TrapGen(q,n) algorithm to generate a pair of matrices $A_0, A_0' \in Z_q^{n\times m}$ and a pair of short (nearly orthogonal) basis $T_{A_0}, T_{A_0'}$ for $\Lambda_q^{\perp}(A_0)$ and $\Lambda_q^{\perp}(A_0')$ such that $\|\widetilde{T_{A_0}}\| \leq O(\sqrt{n \lg q})$ and $\|\widetilde{T_{A_0'}}\| \leq O(\sqrt{n \lg q})$.
2. Select $2l'+1$ random matrices $A_1, A_2, \ldots, A_{l'}$, $A_1', A_2', \ldots, A_{l'}'$ and $D \in Z_q^{n\times m}$ uniformly.
3. Select a random matrix $U \in Z_q^{n\times n}$ uniformly.
4. Finaly it computes master key and the PPs as follows, MK = $(T_{A_0}, T_{A_0'})$, PP = $A_1, A_2, \ldots, A_{l'}, A_1', A_2', \ldots, A_{l'}'$ and $D \in Z_q^{n\times m}, U \in Z_q^{n\times n}$.

5.1.2 Extract(PP, MK, id)

On input PPs (PP), a master secret key (MK), and an identity id = $(b_1, \ldots, b_{l'})$, where each b_i is an $l/l' = \beta$ bit string, algorithm executes following steps.

1. Let $A_{id} = D + \sum_{j=1}^{l'} b_j A_j \ \in Z_q^{n\times m}$.
2. Compute $e \in Z_q^{2m\times n}$ as $e \longleftarrow SampleLeft(A_0, A_{id}, T_{A_0}, U, \sigma)$. Let $E_{id} = (A_0 | A_{id})$, then $E_{id}.e = U$ in $Z_q^{n\times n}$ and e is distributed as $D_{\Lambda_q^u(F_{id}),\sigma}$ by lemma 1.
3. compute $PR_{id} = e \ \in Z^{2m\times n}$.

5.1.3 Enc(PP, id_1, id_2, m)

On input PPs (PP), identities id^{1*}, id^{2*} and a message $m \in \{0,1\}^n$, algorithm executes following steps:

1. Let $A_{id_1} = D + \sum_{j=1}^{l'} b_j A_j \ \in Z_q^{n\times m}$ and $A_{id_2} = D + \sum_{j=1}^{l'} b_j A_j' \ \in Z_q^{n\times m}$.

$$F_{id_1} = (A_0 | A_{id_1}), F_{id_2} = (A_0' | A_{id_2}) \ \in Z_q^{n\times 2m}$$

.

2. Choose a uniformly random $s \xleftarrow{R} Z_q^n$.
3. Choose $2l'$ uniformly random matrices $R_i \xleftarrow{R} \{-1,1\}^{m\times m}$ for $i = 1, \ldots, l'$ and define R_{id_1}[3] $= \sum_{j=1}^{l'} b_j R_j \ \in \{-l'(2^\beta - 1), \ldots, l'(2^\beta - 1)\}$ and $R_{id_2} = \sum_{j=l'+1}^{2l'} b_j R_j \ \in \{-l'(2^\beta - 1), \ldots, l'(2^\beta - 1)\}$.
4. Choose noise vectors $x \xleftarrow{\overline{\Psi}_\alpha} Z_q^n$, $y \xleftarrow{\overline{\Psi}_\alpha^m} Z_q^m$, $z_1 \longleftarrow R_{id_1}^T y \in Z_q^m$ and $z_2 \longleftarrow R_{id_2}^T y \in Z_q^m$.
5. Set $C_0 \longleftarrow U^T s + x + m\lfloor \frac{q}{2} \rfloor \in Z_q^m$, $C_1 = F_{id_1}^T s + \begin{pmatrix} y \\ z_1 \end{pmatrix}$ and $C_2 = F_{id_2}^T s + \begin{pmatrix} y \\ z_2 \end{pmatrix}$.
6. Compute the ciphertext CT = $(C_0, C_1, C_2) \ \in Z_q^n \times Z_q^{2m} \times Z_q^{2m}$.

[3] In provable security proof, R_{id} is used in answering adversary's private key query. Error vector has to be $\begin{pmatrix} y \\ R_{id_i}^T y \end{pmatrix}$

5.1.4 Dec(PP, PR_{id}, CT)

On input PPs (PP), a private key of the i^{th} identity (PR_{id_i}) where $i \in \{1,2\}$, and a ciphertext CT = (C_0, C_1, C_2), algorithm executes following steps.

1. For identity i, compute $w = w_1 w_2 \dots w_n = C_0 - e_{id_i}^T C_i \ \in Z_q^n$.
2. For j = 1 to n
   if $|w_i - \lfloor \frac{q}{2} \rfloor| < \frac{q}{4}$ in Z, $w_i = 1$ else $w_i = 0$.

During Decryption:
$w = C_0 - e_{id_i}^T C_i = b\lfloor \frac{q}{2} \rfloor + x - e_{id_i}^T \begin{bmatrix} y \\ z \end{bmatrix}$.

Correctness After decryption,
Error term $e = e_1 e_2 \dots e_n = x - e_{id}^T \begin{bmatrix} y \\ z_i \end{bmatrix}$ and for correctness IB-DRE scheme each e_i has to be less than $q/4$.

5.1.5 Lemma 5

For an l-bit identity id = $(b_1, \dots, b_{l'})$, where each b_i is $l/l' = \beta$ bit string. The error term's norm is bounded by $q\sigma 2^\beta l' m\alpha\omega(\sqrt{\lg m}) + O(\sigma 2^\beta l' m^{3/2})$.
Proof: The proof of this is similar to the proof of Lemma 22 in [1] except that matrix R is replaced with $R_{id} = \sum_{j=1}^{l'} b_j A_j$. Since $\|R_{id}\| \le \sum_{j=1}^{l'} \|b_j\| \|A_j\|$ and by [1,theorem 15],$\|R\| \le O(\sqrt{m})$.
So $\|R_{id}\| \le O(2^\beta l' \sqrt{m})$.
This leads to an extra factor $2^\beta l'$ in the error bound.

For the scheme to work correctly we have to ensure that:

- Error term $< q/5$ i.e. $\alpha < [\sigma 2^\beta l' m\alpha\omega(\sqrt{\lg m})]^{-1}$ and $q = \Omega(\sigma 2^\beta l' m^{3/2})$.
- $m > 6n \lg q$ to execute TrapGen algorithm.
- That σ is sufficiently large enough for SimpleLeft algorithm and SimpleRight algorithm i.e.

$$\sigma > \|\widetilde{T_D}\| 2^\beta l' \sqrt{m}\omega(\sqrt{\lg m})) = 2^\beta l' \sqrt{m}\omega(\sqrt{\lg m})$$

  .

- that Regev's reduction applies (i.e. $q > 2Q$, where Q is the total number of identity queries asked by the adversary)

To satisfy above requirements we assign the parameters (q, m, σ, α) as follows in terms of security parameter n:

$$\begin{aligned} q &= max(2Q, m^{2.5}(2^\beta l')^2 \omega(\sqrt{\lg n})), \\ \alpha &= [2^\beta l' m\omega(\sqrt{\lg m})]^{-1}. \quad (8) \\ m &= 6n^{1+\delta}, \sigma = 2^\beta l' \sqrt{m}\omega(\sqrt{\lg n}) \end{aligned}$$

From above requirements, we need $q = m^{2.5}(2^\beta l')^2 \omega(\sqrt{\lg n})$. But in [1], required value of $q = m^{2.5} l^2 \omega(\sqrt{\lg n})$. Hence, in this scheme, the value of q is increased by $(2^\beta \frac{l'}{l})^2 = (\frac{2^\beta}{\beta})^2$. This implies that when PPs are reduced by β, q is increased by a factor of $(\frac{2^\beta}{\beta})^2$ or the number of the bits in q is increased by a factor of $(\beta - lg(\beta))^2$.

5.2 Efficiency

Here our time complexity analysis is similar to complexity analysis of [2]. The only difference between the scheme in[4] and our scheme, is the computation of R_{id} and A_{id}. We denote $|Z_q|$ as the size of an element of the set Z_q. A_{id} is computed by adding two matrices of size $n \times m$ and l' multiplication. Here every multiplication is a multiplication of matrix of size $n \times m$ and (l/l')-bit string. Computation cost for every such multiplication is be $(l/l'-1)$ doubling and $l/2l'$ addition. So the total computational cost A_{id} is $(l-l')$ doubling and l/l' addition. Thus complexity of computing A_{id} is equal to $cnm(\frac{3l}{2}-l')|Z_q|$ for some constant c, where $nm|Z_q|$ is computational cost of adding two matrices $(n \times m)$. This computational cost is least when $l' = l$ (as in[4]). Least value is $cnm\frac{l}{2}|Z_q|$. Maximum value is less than $cnm\frac{3l}{2}|Z_q|$. Computational cost of computing $F_{id}^T s$ is equal to $dnmn|Z_q|$ for a constant d. So computational cost of encryption is equal to $cnm(\frac{3l}{2}-l')|Z_q| + dnmn|Z_q|$. Computational cost of encryption in IDBE[4] is equal to $cnm(\frac{l}{2})|Z_q| + dnmn|Z_q|$.
q is less than poly(n) assume n^5. If q is of a value more than 512 bits (value $\approx 2^{512}$) then value of n is atleast 2^{100}, which is much greater than size of identity $l(160)$. So computational cost of encryption is $enmn|Z_q|$ which is independent of l'. It shows that l' does not make any effect on computation of matrix A_{id}. Similarly l' does not make any effect on computation of matrix R_{id}. Hence l' does not make any effect on time complexity of key generation algorithm, encryption algorithm and decryption algorithm. Computational cost is increased because of increase in size of $|Z_q|$ (i.e. value of q).

5.3 Space/Time Trade-Off

The relative reduction in space requirement to store the PPs in our scheme, compared with the scheme in [1] is equal to $\frac{l-l'}{l}$. Our scheme decreases PP by β at the cost of increasing value of prime q by a factor of $(\frac{2^\beta}{\beta})^2$ with same security level as[4]. By making same security level as[4], new q or q' is $q(\frac{2^\beta}{\beta})^2$. Size of $Z_{q'} = |Z_{q'}| = |Z_q| + (\beta - lg(\beta))^2$. Relative increase in encryption cost of our scheme with respect to[4] is $\frac{|Z_{q'}-Z_q|}{|Z_q|} = \frac{(\beta-lg(\beta))^2}{|Z_q|}$.
In table 1, we give the results for $l = 160$ and $|Z_q| = 512$ for various values of l' ranging from 16 to 64. Overall, we suggest $l' = 32$ will be good choice for implementing the scheme.

Table 1. For different values of l', Relative reduction in space and relative rise in time .

l'	Relative reduction in space	Relative rise in time
16	90	8.71
32	80	1.40
64	60	0.27

5.4 Proof

Following abort-resistant hash functions will be required in security proofs.

5.4.1 Abort-Resistant Hash Functions[16].

Definition 6. Suppose function $H = \{\hbar : X \longrightarrow Y\}$ is family of hash functions from X to Y. For a set of $Q+2$ inputs $\bar{x} = (x_0^1, x_0^2, x_1, \ldots, x_Q) \in X^{Q+2}$, the non-abort probability of $\bar{x}$ i.e. $\alpha(\bar{x})$ is as

$$\alpha(\bar{x}) = Pr[\hbar[x_0] = 0 \wedge \hbar[x_1] \neq 0 \wedge \ldots \wedge \hbar[x_Q] \neq 0]$$

Here the probability is computed over the random choice of $\hbar$ in H.
We say that H is $(Q, \alpha_{min}, \alpha_{max})$ abort-resistance if for all $\bar{x} = (x_0^1, x_0^2, x_1, \ldots, x_Q) \in X^{Q+2}$ with $x_0^1, x_0^2 \notin$

$\{x_1,\ldots,x_Q\}$ we have $\alpha(\bar{x}) \in [\alpha_{min}, \alpha_{max}]$.
Following abort-resistant hash family is used which is very similar to [16].
For a q (prime) let $(Z_q^{l'})^* = Z_q^{l'} - \{0^l\}$ and hash function family defined as

$$H : \{\hbar : ((Z_q^{l'})^*) \longrightarrow (Z_q)\}$$

$$\hbar(id) = (1 + \sum_{j=1}^{l'} h_j b_j) \in Z_q \tag{9}$$

where h_i and b_i are defined in section 4.1.

5.4.2 Lemma 6

The Hash family H, as defined in (4) is $(Q, \frac{1}{q}(1-\frac{Q}{q}), \frac{1}{q})$ abort-resistant where prime q is greater than $Q > 0$.
Proof: The proof of this is very similar to [1]. Consider a set of $\overline{id}$ of $Q+2$ inputs $id_0^1, id_0^2, \ldots, id_Q$ in $(Z_q^{l'})^*$ where $id_0 \notin \{id_1,\ldots,id_Q\}$. For $i = 0,\ldots,Q+1$ let S_i be the set of functions $\hbar$ in H where $\hbar(id_i) = 0$.
We know that number of such functions $= |S_i| = \frac{(q2^\beta)^{l'}}{q}$.
And $|S_0^1 \wedge S_0^2 \wedge S_j| \leq \frac{(q2^\beta)^{l'}}{q^3}$ for every $j > 0$. Number of functions in H such that $\hbar(id_0) = 0$ but $\hbar(id_i) \neq 0$ for $i = 1,\ldots,Q$. $= |S|$ and

$$|S| = |S_0^1 \wedge S_0^2 - (S_1 \wedge, \ldots, S_Q)| \geq |S_0^1 \wedge S_0^2| - \sum_{j=1}^{Q} |S_0^1 \wedge S_0^2 \wedge S_j|$$

$$\geq \frac{(q2^\beta)^{l'}}{q^2} - Q\frac{(q2^\beta)^{l'}}{q^3}$$

Since number of functions in $H = (q2^\beta)^{l'}$, therefore the no-abort probability of identities would be equal to atleast $\frac{\frac{(q2^\beta)^{l'}}{q^2} - Q\frac{(q2^\beta)^{l'}}{q^3}}{(q2^\beta)^{l'}} = \frac{1}{q^2}(1-\frac{Q}{q})$
Since $|S| \leq |S_0^1 \wedge S_0^2|$, so the no-abort probability is atmost $\frac{|S_0^1 \wedge S_0^2|}{(q2^\beta)^{l'}} = \frac{1}{q^2}$.

Now we show that our lattice-based IB-DRE construction cannot be distinguished from random under a adaptive identity attack (IND-ID-CPA).

Theorem 5.1. *The Full IB-DRE scheme with parameters$(q,n,m,\overline{\sigma},\overline{\alpha})$ as in (3) is IND-ID-CPA secure provided that the $(Z_q,n,\bar{\Psi}_{\alpha_d})$-LWE assumptions hold.*

Proof The proof of this is similar to[16, 3]. We will show that if there exists a Probabilistic Polynomial-Time (PPT) adversary $\mathscr{A}$ that breaks our $IB-DRE$ scheme in polynomial time with non-negligible probability then there exists a Probabilistic Polynomial-Time challenger $\mathscr{B}$ that would answer whether an oracle O (unspecified challenge) is either a truly random sampler $O_\$$ or a noisy pseudo-random sampler O_s by simulating views of adversary $\mathscr{A}$ (solves the LWE problem).

Setup Challenger $\mathscr{B}$ generates random matrix $A_0 \in Z_q^{n\times m}$ uniformly . Using TrapGen algorithm, random matrix D in $Z_q^{n\times m}$ and a Trapdoor T_D for $\Lambda_q^{\perp}(D)$ is generated. Challenger also chooses l'' uniformly random matrices $R_i \in [-1,1]^{m\times m}, i \in [1,l']$ and l' random scalars $h_i \in Z_q, i \in [1,l']$. Next it constructs the matrices A_i as

$$A_i \longleftarrow A_0 R_i + h_i D$$

By lemma 2, the distribution of A_i's are statistically close to the uniform distribution.

$$F_{id} = \left(A_0 | \sum_{j=1}^{l'} A_j b_j + D \right) \tag{10}$$

From equation (6), substituting the matrices A_i' s value we get

$$F_{id} = (A_0 | A_0 R_{id} + D h_{id})$$

where $R_{id} = \sum_{j=1}^{l'} R_j b_j$ and $D_{id} = D\hbar_{id} = D(1 + \sum_{j=1}^{l'} h_j b_j)$
If $\hbar_{id}$ is equal to zero then challenger will not be able to answer the private key query and it will be part of abort resistant hash function.
Else if $\hbar_{id} \neq 0$ then challenger $\mathscr{B}$ answers the secret key query of id by running

$$PR_{id} \longleftarrow \text{SampleRight}(A_0, D_{id}, R_{id}, T_D, 0, \sigma_l)$$

and sending PR_{id} to A.

Challenge Adversary declares target identities id_1^* and id_2^*. Challenger B gets 3 LWE samples i.e. $(U_i, u_i) \in Z_q^{n\times n} \times Z_q^n$ $(0 \leq i \leq 2$ from an oracle.

1. Blind the message $m \in \{0,1\}^n$ by letting

$$C_0^* = u_0 + m^* \lfloor \frac{q}{2} \rceil \in Z_q$$

2. Challenger also chooses l'' uniformly random matrices $R_i^* \in [-1,l]^{m\times m}, i \in [1,l'']$. Let

$$R_{id^*} = (R_1^* | \ldots | R_{l''}^*)$$

and set

$$C_1^* = \begin{pmatrix} v_1^* \\ (R_{id^*})^T v_1^* \end{pmatrix} \in Z_q^{m+l''m}$$

and

$$C_2^* = \begin{pmatrix} v_2^* \\ (R_{id^*})^T v_2^* \end{pmatrix} \in Z_q^{m+l''m}$$

3. Choose a random bit $r \leftarrow \{0,1\}$. If $r = 0$, send $CT^* = (C_0^*, C_1^*, C_2^*)$ to the adversary. If $r = 1$ choose a random $(C_0, C_1, C_2) \in Z_q \times Z_q^{m+l''m}$ and send (C_0, C_1, C_2) to the adversary.

Phase 2 Except id^* and prefix of id^*, adversary can make private key query for any id. Simulator repeats the same method used in Setup() part to answer the query.

Since, for non-abort probability $h_{id^*} = 0$ then $F_{id^*} = (A_0|A_0\overline{R}_{id^*})$. When the LWE oracle is pseudorandom

$$v^* = A_0^T s + y$$

for some random noise $y \in Z_q^m$ distributed as $\bar{\psi}_\alpha^m$. Therefore

$$C_1^* = \begin{pmatrix} A_0^T s + y \\ (A_0 R_{id^*})^T s + (R_{id^*})^T y \end{pmatrix} = (F_{id^*})^T s + \begin{pmatrix} y \\ (R_{id^*})^T y \end{pmatrix}$$

Above C_1^* is a valid C_1 part of ciphertext challenge. Again $C_0^* = u_0^T + x + b^* \lfloor \frac{q}{2} \rceil$ is also a valid C_0 part of challenge ciphertext. Therefore (C_0^*, C_1^*) is valid challenge ciphertext.
Similar to proof of theorem 4.1, there exists PPT algorithm $\mathscr{B}$ that solves the $(Z_q, n, \overline{\psi}_\alpha)$-LWE problem with $\varepsilon' \geq \varepsilon/4q^{2l}$ in about the time $= t_1 + O(\varepsilon^{-2} ln(\varepsilon^{-1})\lambda ln(\lambda^{-1}))$. Since no one can solve LWE hard problem so our scheme is also semantically secure.

6 Conclusion

Both the schemes has been proved to be IND-CPA (semantically) secure on lattice based hard problem i.e LWE. PPs in our schemes can be further improved by converting them to ideal lattices. It has been shown in theorem that converting to adaptive-ID HIB-DRE from selective-ID HIB-DRE security degradation is q^l (exponential). The main open problem is to design adaptive-ID HIB-DRE secure scheme without exponential degradation. In our IB-DRE scheme we have also presented that there exists a trade-off between the reduction in the PP size and the increase in the time complexity (cost of computation) i.e. value of q. It will be interesting to design IB-DRE scheme from latices with short (nearly orthogonal) PP without an increase in the value of q (i.e., cost of computation).

References

[1] David Naccache. Secure and Practical identity-based encryption. Cryptology ePrint Archive, Paper 2005/369, 2005. `https://eprint.iacr.org/2005/369` [Online; accessed on November 03, 2022].

[2] S. Chatterjee and P. Sarkar. Trading Time for Space: Towards an Efficient IBE Scheme with Short(er) Public Parameters in the Standard Model. In *Proc. of the 8th International Conference on Information Security and Cryptology (ICISC'05), Seoul, Korea*, volume 3935 of *Lecture Notes in Computer Science*, pages 424–440. Springer, Berlin, Heidelberg, 2005.

[3] K. Singh, P. Rangan, and A.K. Banerjee. Adaptively Secure Efficient Lattice (H)IBE in Standard Model with Short Public Parameters. In *Proc. of the 2nd International Conference on Security, Privacy and Applied Cryptography Engineering (SPACE'12), Chennai, India*, volume 7644 of *Lecture Notes in Computer Science*, pages 153–172. Springer, Berlin, Heidelberg, November 2012.

[4] D. Zhang, K. Zhang, B. Li, X. Lu, and H. Xue. Lattice-Based Dual Receiver Encryption and More. In *Proc. of the 23rd Australasian Conference on Information Security and Privacy (ACISP'18), Wollongong, New South Wales, Australia*, volume 10946 of *Lecture Notes in Computer Science*, pages 520–538. Springer, Cham, July 2012.

[5] T. Diament, H.K.. Lee, A.D. Keromytis, and M. Yung. The dual receiver cryptosystem and its applications. In *Proc. of the 11th ACM Conference on Computer and Communications Security (CCS'04), Washington DC, USA*, pages 330–343. ACM, October 2004.

[6] S.S.M. Chow, M.K. Franklin, and H. Zhang. Practical dual-receiver encryption - soundness, complete non-malleability, and applications. In *Proc. of the Cryptographer's Track at the RSA Conference 2014 (CT-RSA'14), San Francisco, California, USA*, volume 8366 of *Lecture Notes in Computer Science*, pages 85–105. Springer, Cham, February 2014.

[7] W.P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997.

[8] M. Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proc. of the 28th annual ACM symposium on Theory of Computing (STOC'96), Philadelphia, Pennsylvania, USA*, pages 99–108. ACM, July 1996.

[9] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proc. of the 37th annual ACM symposium on Theory of Computing (STOC'05), Baltimore, Maryland, USA*, pages 84–93. ACM, May 2005.

[10] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, November 1979.

[11] C. Cocks. An identity based encryption scheme based on quadratic residues. In *Proc. of the 8th IMA International Conference on Cryptography and Coding (IMACC'01), Cirencester, UK*, volume 2260 of *Lecture Notes in Computer Science*, pages 360–363. Springer, Berlin, Heidelberg, December 2001.

[12] D. Boneh and K.M. Franklin. Identity based encryption from the weil pairing. In *Proc. of the 21st Annual International Cryptology Conference (CRYPTO'01), Santa Barbara, California, USA*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer, Berlin, Heidelberg, August 2001.

[13] C. Gentry and A. Silverberg. Hierarchical id-based cryptography. In *Proc. of the 8th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'02), Queenstown, New Zealand*, volume 2501 of *Lecture Notes in Computer Science*, pages 548–566. Springer, Berlin, Heidelberg, December 2002.

[14] J. Horwitz and B. Lynn. Toward hierarchical identity-based encryption. In *Proc. of the 2002 International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'02), Amsterdam, The Netherlands*, volume 2332 of *Lecture Notes in Computer Science*, pages 466–481. Springer, Berlin, Heidelberg, April-May 2002.

[15] D. Boneh and X. Boyen. Secure identity based encryption without random oracles. In *Proc. of the 24th Annual International Cryptology Conference (CRYPTO'04), Santa Barbara, California, USA*, volume 3152 of *Lecture Notes in Computer Science*, pages 443–459. Springer, Berlin, Heidelberg, August 2004.

[16] S. Agrawal, D. Boneh, and X. Boyen. Efficient lattice (h)ibe in the standard model. In *Proc. of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'10), French Riviera*, volume 6110 of *Lecture Notes in Computer Science*, pages 553–572. Springer Berlin, Heidelberg, May-June 2010.

[17] K. Singh, P. Rangan, and AK. Banerjee. Efficient lattice hibe in the standard model with shorter public parameters. In *Proc. of the 2nd IFIP TC 5/8 International Conference on Information and Communication Technology (ICT-EurAsia'14), Bali, Indonesia*, volume 8407 of *Lecture Notes in Computer Science*, pages 542–553. Springer Berlin, Heidelberg, April 2014.

[18] A. Georgescu. Anonymous lattice-based broadcast encryption. In *Proc. of the 2013 International Conference on Information and Communication Technology (ICT-EurAsia'13), Yogyakarta, Indonesia*, volume 7804 of *Lecture Notes in Computer Science*, pages 353–362. Springer Berlin, Heidelberg, March 2013.

[19] K. Hoffman and R. Kunze. *Linear Algebra*. Prentice-Hall, Inc., 1971.

[20] K. Singh, P. Rangan, and AK. Banerjee. Lattice forward-secure identity based encryption scheme. *Journal of Internet Services and Information Security*, 2(3/4):118–128, November 2012.

[21] D. Micciancio and S. Golwasser. *Complexity of Lattice Problems: A Cryptographic Perspective*. Springer New York, 2002.

[22] J. Alwen and C. Peikert. Generating shorter bases for hard random lattices. In *Proc. of the 26th International Symposium on Theoretical Aspects of Computer Science (STACS'09), Freiburg, Germany*, pages 75–86. IBFI Schloss Dagstuhl, February 2009.

[23] B. Applebaum, D. Cash, C. Peikert, and A. Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In *Proc. of the 29th Annual International Cryptology Conference (CRYPTO'09), Santa Barbara, California, USA*, volume 5677 of *Lecture Notes in Computer Science*, pages 595–618. Springer, Berlin, Heidelberg, August 2009.

[24] R. Lindner and C. Peikert. Better key sizes (and attacks) for lwe-based encryption. In *Proc. of the Cryptographers' Track at the RSA Conference 2011 (CT-RSA'11), San Francisco, California, USA*, volume 6558 of

Lecture Notes in Computer Science, pages 319–339. Springer Berlin, Heidelberg, February 2011.

[25] R.B. Waters. Efficient identity-based encryption without random oracles. In *Proc. of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'05), Aarhus, Denmark*, volume 3494 of *Lecture Notes in Computer Science*, pages 114–127. Springer Berlin, Heidelberg, May 2005.

[26] S. Chatterjee and P. Sarkar. Hibe with short(er) public parameters without random oracle. In *Proc. of the 12th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'06), Shanghai, China*, volume 4284 of *Lecture Notes in Computer Science*, pages 145–160. Springer Berlin, Heidelberg, December 2006.

[27] M. Bellare and M. Ristenpart. Simulation without the artificial abort: Simplified proof and improved concrete security for waters' ibe scheme. In *Proc. of the 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'09), Cologne, Germany*, volume 5479 of *Lecture Notes in Computer Science*, pages 407–424. Springer Berlin, Heidelberg, April 2009.

Author Biography

Kunwar Singh received his B.Tech. degree from IIT Delhi, his M.Tech. degree from Jawaharlal University, New Delhi and his Ph.D. degree from IIT Madras in 2015. Currently, he is an Assistant Professor in the Department of Computer Science and Engineering at National Institute of Technology - Trichy (NITT), India since 2006. His areas of research include Public Key Cryptography, Identity-Based Encryption, Lattice Based Cryptography, Stream Ciphers, Multi-party Computation and Blockchain.

C. Pandu Rangan is Visiting Chair Professor in Division of Electrical, Electronics, and Computer Science (EECS) of Indian Institute of Science (IISc). C. Pandu Rangan is a professor in the department of computer science and engineering of Indian Institute of Technology - Madras, Chennai, India. His areas of interest are in theoretical computer science mainly focusing on Cryptography, Algorithms and Data Structures, Game Theory, Graph Theory and Distributed Computing.

Ilsun You (Senior Member, IEEE) Dr. Ilsun YOU received the MS and PhD degrees in computer science from Dankook University, Seoul, Korea, in 1997 and 2002, respectively. He received the second PhD degree from Kyushu University, Japan, in 2012. Now, he is a full professor at Department of Information Security, Cryptology, and Mathematics, Kookmin University. He has served or is currently serving as a Steering Chair, General Chair or a Program Chair of international conferences and symposiums such as MobiSec'16-21, WISA'19-20, ProvSec'18, ACM MIST'15-17 and so forth. Dr. YOU has focused on 5/6G security, security for wireless networks mobile internet, IoT/CPS security and so forth while publishing more than 180 papers in these areas. He is a Fellow of the IET and a Senior member of the IEEE.

Amalan Joseph Antony received the Bachelor's degree (with distinction) in Electronics and Communication Engineering from PSG College of Technology, Coimbatore, India, in 2010, and the Master's degree (with distinction) in Computer Science and Engineering from the National Institute of Technology, Tiruchirappalli, India, in 2019. Currently he leads the Software and Application Development Section of the Computer Centre at the National Institute of Technology, Tiruchirappalli, India, and is working toward the PhD degree at the National Institute of Technology, Tiruchirappalli, India. His research interests include Cryptography, Blockchain, Zero-knowledge proof, and Secure multi-party computation.

SK Karthika received her M. Tech degree in University College of Engineering, Trichy Campus. Currently she is working as Senior Research Fellow at National Institute of Technology, Tiruchirappalli, under the project "Research and Development of Lightweight Stream Ciphers" sponsored by Department of Science and Technology, India. Also, she is pursuing PhD under the guidance of Dr. Kunwar Singh. Her area of research is cryptanalysis and Stream ciphers.

Jiyoon Kim received the Ph.D. degrees in information security from Soonchunhyang University, Asan, South Korea, in 2022. He is currently working as a Assistant Professor with the Department of Computer Science, Gyeongsang National University, Jinju, South Korea. His main research interests include 5G/6G security and formal security analysis.