Maximum Leakage Resilient IBE and IPE under the DLIN assumption

Kaoru Kurosawa[1] and Le Trieu Phong[2]

[1] Ibaraki University
[2] NICT, Japan

Abstract. In this paper, we show identity-based encryption (IBE) and inner product encryption (IPE) schemes which achieve the maximum-possible leakage rate $1 - o(1)$. These schemes are secure under the decision linear (DLIN) assumption in the standard model. Specifically, even if $1 - o(1)$ fraction of each private key is arbitrarily leaked, the IBE scheme is fully secure and the IPE scheme is selectively secure. (To our knowledge, no *leakage resilient* IPE scheme has been known so far.) Moreover, their variants with leakage rate $1/2 - o(1)$ enjoy comparable private keys and ciphertexts with the counterparts without leakage resilience in the literature.

Keywords: Identity-based encryption, inner product encryption, leakage resilience, DLIN assumption.

1 Introduction

1.1 Background

Leakage-resilient cryptography tries to deal with the question: "Can we do cryptography with *no perfect* secrets?". The question is natural, since generating and handling secrets is uneasy in practice, and furthermore they can be leaked by side-channel attacks. Following the research trend, in this paper we will focus on leakage resilient IBE, and IPE schemes, in which identities' private keys may be arbitrarily leaked for one time. That is, we will work in the bounded leakage model of [3].

Recall that in identity-based encryption, first proposed by Shamir [24], one can use arbitrary strings as public keys. The research on IBE is an active and stimulating field of cryptography, and so far IBE schemes have been constructed under several assumptions: pairing-related assumptions, quadratic residue-related assumptions and lattice-related assumptions. Akavia et al. [3] and Alwen et al. [4, 5] showed that some variants of them are secure against private key leakage attacks. The security of these schemes is either analyzed in the random oracle model or is based on "non-static" assumption in the standard model. In the standard model, Chow et al. [13] presented a leakage resilient IBE with the leakage rate 1/3 under the DBDH assumption. Above and below, the leakage rate is defined as the fraction of

$$\frac{\text{size of leakage permitted}}{\text{size of private key}}.$$

Also recall that inner product encryption [16] goes beyond IBE by allowing encryption under attribute vectors, while private keys are associated with predicate vectors. Let u be an encryption attribute vector, and id a predicate vector, then decryption works correctly if the inner product $\langle id, u\rangle = 0$. IPE implies IBE, since to test $id_{\rm IBE} = id'_{\rm IBE}$ for some identities $id_{\rm IBE}$ and $id'_{\rm IBE}$, just check whether the inner product between vectors $id = (1, id_{\rm IBE})$ and $u = (id'_{\rm IBE}, -1)$ equals 0. IPE also serves as an important tool for designing encryption scheme supporting queries on encrypted data [11], and disjunctions, polynomial evaluation [16]. IPE is a class of functional encryption, which is a very active research field thanks to their potentially-wide applications.

Recently IPE (and hence IBE) have been realized under the DLIN assumption. This assumption, first formalized in [9], is very appealing and has been used in various works. In particular, Okamoto and Takashima [21] showed a general functional encryption scheme under DLIN. As a special case of their IPE scheme, an IBE scheme is obtained such that ciphertexts and keys consist of 8 group elements. Lewko [17] gets the sizes to 6 group elements. Bellare et al. [6] further reduce the sizes to 5 elements for ciphertexts, and 4 for private keys.

Table 1. Leakage resilient IBE in the standard model under static assumptions.

IBE Schemes	Assumption	Ciphertext overhead (group elements)	Private key (group elements)	Memory leakage rate
Chow et al. [13]	DBDH	$\|\mathsf{seed}\| + 3$	3	$1/3$
Lewko et al. [19]	$1, 2, 3$	L	L	$\frac{1}{1+c_1+c_3}(1 - O(1/L))$
Ours (Sect.3)	DLIN	2ℓ	2ℓ	$1 - \frac{3}{2\ell} - o(1)$
		6	6	$1/2 - o(1)$

Above, $c_1 = |p_1|/|p_2|, c_3 = |p_3|/|p_2|$ for some primes p_1, p_2, p_3, and $L \geq 4$, $\ell \geq 3$. The elements may belong to different groups, but we ignore that for simplicity. Assumptions $1, 2, 3$ are some new assumptions in composite bilinear groups (see [19] for details).

Also under the DLIN assumption, Bellare, Waters, and Yilek [8] gave an IBE which is secure against the selective opening attack. Their scheme encrypts one bit and is not in any leakage-resilient model.

Thus in the literature, under the DLIN assumption,

- **On IBE:** No fully-secure, efficient, leakage-resilient IBE is known to achieve the maximum-possible leakage rate $1 - o(1)$.
- **On IPE:** While IPE is considerably examined recently, e.g. via [2, 16, 18, 21, 22], the case of *leakage resilient* IPE is still poorly understood. To our knowledge, no leakage resilient IPE scheme is proposed so far.

1.2 Our contributions

Results on IBE. In this paper, we show the first leakage resilient IBE which achieves the maximum-possible leakage rate $1 - o(1)$ in the standard model under a static assumption. That is, it is fully secure under under the DLIN assumption even if $1 - o(1)$ fraction of each private key is arbitrarily leaked. We do not use randomness extractors, as opposed to most of the known leakage resilient schemes. Precise values are in Table 1.

Setting minimal $\ell = 3$ in Table 1, we obtain an instantiation with leakage rate $1/2 - o(1)$. The ciphertext overhead is only 6 group elements, and the private key also consists of only 6 group elements.

Note also in Table 1, the IBE in Lewko et al. [19], while tolerating master key leakage, has private key leakage rate $\frac{1}{1+c}(1 - o(1))$ for $c > 0$. This rate cannot reach $1 - o(1)$ simply because c cannot be 0 (see the caption of Table 1).

Technically, from the viewpoint of leakage resilience, our KEMs are based on the leakage resilient public key encryption scheme of Naor and Segev [20]. From the viewpoint of utilizing trapdoor in security reduction, our KEMs are motivated from the lattice based IBE of Agrawal, Boneh, and Boyen [1].

Results on IPE. Going further, we propose the *first* leakage resilient IPE scheme in the literature. The scheme is selectively-secure, under the DLIN assumption, with private key leakage rate $1 - \frac{3}{2\ell} - o(1)$. Each private key consists of 2ℓ group elements, while the ciphertext overhead is of $(n + 1)\ell$ group elements where n is the length of attributes. Taking $\ell = 3$ yields an instantiation with constant private key size of only 6 group elements, ciphertext overhead of $3n + 3$ group elements, with leakage rate $1/2 - o(1)$.

The design of our IPE scheme is partially inspired by the work of Agrawal et al. [2] in the lattice setting. Curiously, the lattice-based scheme is not known to be leakage resilient.

Roadmap. Section 3 is for IBE, while Section 4 is for IPE. To illustrate the main ideas, we start with a simple IBE scheme, which is selectively-secure and leakage-resilient, in Sect.3.1. We then show how to modify the scheme to obtain a fully-secure one in Sect.3.2. The IPE scheme is in Sect.4.

More related works. Above we have discussed related works in which the private keys are leaked, while arbitrarily, but once. There are works on IBE considering stronger model of leakage. In particular, Brakerski et al. [12] considered the continual memory leakage model, and presented a selective secure IBE scheme. Yuen et al. [26] generalized that to the continual auxiliary input model, and proposed an IBE scheme fully secure under three static assumptions in composite order pairing groups.

2 Preliminaries

Notations. Denote $a \xleftarrow{\$} A$ as the process of taking a randomly from a set A. Let $|a|$ be the bit length of the element a, while $|A|$ be the order of the set. Let q be a prime. We call $\mathbb{PG} = (\mathbb{G}, \mathbb{G}_T, g, \hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T)$ a pairing group if $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic groups of order q. The element g is a generator of $\mathbb{G}$, and the mapping $\hat{e}$ satisfies the following properties: $\hat{e}(g,g) \neq 1$, and $\hat{e}(g^a, g^b) = \hat{e}(g,g)^{ab}$.

Vectors and matrices will be in boldface. Let $\mathbb{Z}_q^{m\times n}$ be the matrices of size $m \times n$ over $\mathbb{Z}_q$. For an integer $r > 0$, the set $\mathrm{Rk}_r(\mathbb{Z}_q^{m\times n})$ contains matrices of rank r in $\mathbb{Z}_q^{m\times n}$. For a matrix $\mathbf{A}$ over $\mathbb{Z}_q$, let $g^{\mathbf{A}} = \left(g^{\mathbf{A}[i,j]}\right)$, which is a matrix over $\mathbb{G}$. Also for the matrix $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$, $\mathrm{span}(\mathbf{A}) = \{\mathbf{zA} : \mathbf{z} \in \mathbb{Z}_q^{1\times m}\}$, while $\ker(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}_q^{n\times 1} : \mathbf{A}\cdot\mathbf{x} = \mathbf{0}\}$.

DLIN assumption. The decision linear assumption, originated in [9], essentially says that given g_1^x and g_2^y, it's hard to distinguish g^{x+y} from random, where $x, y \xleftarrow{\$} \mathbb{Z}_q$, and $g_1, g_2, g \xleftarrow{\$} \mathbb{G}$.

For our purpose, we will consider the matrix $g^{\mathbf{A}}$ where $\mathbf{A} \in \mathbb{Z}_q^{3\times\ell}$ for $\ell \geq 3$ of rank either 2 or 3. If the DLIN assumption holds, then given $g^{\mathbf{A}}$, it is hard to tell the rank of $\mathbf{A}$. (See [20, full version] for a more general result.) More precisely, for any poly-time distinguisher $\mathcal{D}$, the advantage

$$\left|\Pr\left[b' = b : \begin{array}{l}\mathbf{A}_0 \xleftarrow{\$} \mathrm{Rk}_2(\mathbb{Z}_q^{3\times\ell}), \mathbf{A}_1 \xleftarrow{\$} \mathrm{Rk}_3(\mathbb{Z}_q^{3\times\ell}),\\ b \xleftarrow{\$} \{0,1\}, b' \leftarrow \mathcal{D}(g, g^{\mathbf{A}_b})\end{array}\right] - \frac{1}{2}\right|$$

is negligible under the DLIN assumption.

IBE and its security definitions. The scheme consists of algorithms (Setup, $\mathsf{Extract}$, Enc, Dec). Setup generates the public parameters and master key (pp, msk). The public pp is the input to all other algorithms. $\mathsf{Extract}$, on input msk and an identity id, returns the private key sk_{id}. Enc, on input id and a message m, returns a ciphertext c, which will be decrypted by an identity holding sk_{id}, yielding m.

We now recap both the leakage-resilient IND-sID-CPA security. Below, $0 < \rho_M < 1$ stands for the memory leakage rate. Maximum rate means $\rho_M = 1 - o(1)$, at which we aim.

Definition 1 (Leakage resilient IND-sID-CPA security). *An IBE scheme is IND-sID-CPA secure with leakage rate ρ_M if any poly-time adversary succeeds in the following game with probability negligibly close to $1/2$.*

1. **Identity selection:** *the adversary decides and sends the target identity id^* to the challenger.*
2. **Setup***: the challenger runs Setup to generate (msk, pp), and sends pp to the adversary.*
3. **Private key generation:** *the challenger runs $sk_{id^*} \leftarrow \mathsf{Extract}(msk, id^*)$.*
4. **Query set 1:** *the adversary makes queries of the following types:*
   - *Extract queries id for $id \neq id^*$. The challenger returns $sk_{id} = \mathsf{Extract}(msk, id)$ to the adversary.*
   - *Leakage queries (leak_i, id) where id can be id^*, and leak_i is a function. The challenger returns $\mathsf{leak}_i(sk_{id})$ to the adversary. These queries can be adaptive, and it is required that the sum of all lengths $|\mathsf{leak}_i(sk_{id})|$ $(i \geq 1)$ is less than $\rho_M|sk_{id}|$.*
   - *Reveal queries id: if $id \neq id^*$ was in a leakage query, namely sk_{id} was partially leaked, the adversary can even ask for the whole sk_{id}.*
5. **Challenge:** *the adversary gives equal-length m_0, m_1 to the challenger, who computes and sends back $c^* \leftarrow \mathsf{Enc}(id^*, m_b)$ for $b \xleftarrow{\$} \{0,1\}$.*

6. **Query set 2:** *the adversary issues additional extract queries id with* $id \neq id^*$ *to which the challenger answers in the same manner as above.*
7. **Finish:** *the adversary outputs a guess* $b' \in \{0,1\}$*. It succeeds if* $b' = b$*.*

Definition 2 (Leakage resilient IND-ID-CPA security). *An IBE scheme is IND-ID-CPA secure with leakage rate* ρ_M *if any poly-time adversary succeeds in the following game with probability negligibly close to* $1/2$*.*

1. **Setup***: the challenger runs* Setup *to generate* (msk, pp)*, and sends pp to the adversary.*
2. **Query set 1:** *the adversary makes queries of the following types:*
   - *Extract queries id. The challenger returns the private key* $sk_{id} = \mathsf{Extract}(msk, id)$ *to the adversary.*
   - *Leakage queries* (leak_i, id) *where* leak_i *is a function. The challenger returns* $\mathsf{leak}_i(sk_{id})$ *to the adversary.*
   - *Reveal queries id: if id was in a leakage query, namely* sk_{id} *was partially leaked, the adversary can even ask for the whole* sk_{id}*.*
3. **Identity selection:** *the adversary decides and send the target identity* id^* *to the challenger. It is possible that* id^* *was appeared at leakage queries above, but not at reveal or extract queries.*
4. **Query set 2:** *same as query set 1 above, except there is no extract or reveal query on* id^**.*
   It is required that the sum of all lengths $|\mathsf{leak}_i(sk_{id})|$ $(i \geq 1)$ *is less than* $\rho_M |sk_{id}|$*.*
5. **Challenge:** *The adversary gives equal-length* m_0, m_1 *to the challenger, who computes and sends back* $c^* \leftarrow \mathsf{Enc}(id^*, m_b)$ *for* $b \xleftarrow{\$} \{0,1\}$*.*
6. **Query set 3:** *the adversary can ask more of extract queries* $id \neq id^*$*.*
7. **Finish:** *the adversary outputs a guess* $b' \in \{0,1\}$*. It succeeds if* $b' = b$*.*

Removing leakage queries (and hence reveal queries) from the above definitions gives us the standard security definitions for IBE.

Inner product encryption. Consider algorithms $(\mathsf{Setup}, \mathsf{Extract}, \mathsf{Enc}, \mathsf{Dec})$ as in the IBE case. Here $\mathsf{Extract}(msk, id)$ produces a key sk_{id}, while $\mathsf{Enc}(u, m)$ with attribute u returns a ciphertext c of the message m. Decryption $\mathsf{Dec}(id, sk_{id}, c)$ works correctly if the inner product, defined over some group, between id and u is 0, namely $\langle id, u \rangle = 0$. Define $\mathsf{Pred}_{id}(u) = \texttt{true}$ (resp, $\texttt{false}$) iff $\langle id, u \rangle = 0$ (resp, $\neq 0$). Leakage resilient, selective security for IPE schemes are defined as follows.

Definition 3 (Selectively secure IPE, with private key leakage). *An IPE scheme is leakage resilient, selectively secure if the advantage of any poly-time adversary* $\mathcal{A}$ *is negligible in the following game.*

1. **Target:** $\mathcal{A}$ *announces attributes* $u^{(0)}$*,* $u^{(1)}$*.*
2. **Setup:** $(mpk, msk) \leftarrow \mathsf{Setup}$*, and mpk is given to* $\mathcal{A}$*.*
3. **Phase 1:** $\mathcal{A}$ *can ask extract query id to get* sk_{id} *as long as* $\mathsf{Pred}_{id}(u^{(0)}) = \mathsf{Pred}_{id}(u^{(1)}) = \texttt{false}$*.*
   $\mathcal{A}$ *can also ask* (leak_i, id) *to obtain leakage* $\mathsf{leak}_i(sk_{id})$ *where id satisfies the same restriction. The condition is that the total length of all* $|\mathsf{leak}_i(id)|$ *is less than* $\rho_M |sk_{id}|$ *for each id.*
   Moreover, if $\mathcal{A}$ *has already asked extract query id, it will not ask for leakage on the same id (since doing so yields no more advantage to* $\mathcal{A}$*). On the other hand, if id was appeared in a leakage query, it can later be used in an extract query.*
4. **Challenge:** $\mathcal{A}$ *submits equal-length* $m^{(0)}, m^{(1)}$ *for encryption. The challenger takes* $b \xleftarrow{\$} \{0,1\}$*, and sets* $c^* = \mathsf{Enc}(u^{(b)}, m^{(b)})$*.*
5. **Phase 2:** $\mathcal{A}$ *can ask for more extract queries as in Phase* 1*, with the same restriction as in challenge phase.*
6. **Guess:** $\mathcal{A}$ *return* b' *as a guess of* b*. Its advantage is defined as* $|\Pr[b' = b] - 1/2|$*.*

We above assume that $\mathsf{Pred}_{id}(u^{(0)}) = \mathsf{Pred}_{id}(u^{(1)}) = \texttt{false}$ for all extract and leakage queries id. The same restriction was also made in [2, 18, 21]. This is slightly stronger than [16].

Generalized leftover hash lemma. A family of hash function $\mathcal{H} = \{h : X \to Y\}$ is called universal if $\Pr_{h \xleftarrow{\$} \mathcal{H}}[h(x) = h(x')] = 1/|Y|$ for all $x \neq x' \in X$. Let U_Y be the uniform distribution on Y. We will make use of the following lemma.

Lemma 1 (cf. [1]) *Let $\mathcal{H} = \{h : X \to Y\}$ be a universal hash family. Let $f : X \to Z$ be some function. Then for any random variable T taking values in X, the statistical distance*

$$\Delta\Big((h, h(T), f(T)); (h, \mathsf{U}_Y, f(T))\Big) \leq \frac{1}{2}\sqrt{\gamma(T) \cdot |Y| \cdot |Z|},$$

where $\gamma(T) = \max_t \Pr[T = t]$. In other words, if the right-hand side is negligible, $h(T)$ is almost random even given h and the side information $f(T)$.

3 Proposed IBE schemes under DLIN

We begin with a basic IBE scheme to illustrate the main ideas. Then we show how to extend the basic one to a fully secure scheme. From the viewpoint of utilizing trapdoor in security reduction, our IBE schemes are motivated from the lattice-based IBE of Agrawal, Boneh, and Boyen [1]. Perhaps surprisingly, a big difference from [1] is that we achieve the maximum possible leakage rate $1 - o(1)$, while the counterparts in [1] are not leakage resilient.

3.1 Basic scheme: selectively secure IBE

– Setup: Fix $\ell \geq 3$. The public parameters are $pp = (g^{\mathbf{A}_0}, g^{\mathbf{A}_1}, \mathbf{B}, g^{\mathbf{D}})$, where the matrices $\mathbf{A}_0$, $\mathbf{A}_1$, $\mathbf{B} \xleftarrow{\$} \mathbb{Z}_q^{2\times\ell}$ and $\mathbf{D} \xleftarrow{\$} \mathbb{Z}_q^{2\times 1}$. The master secret key is $msk = (\mathbf{A}_0, \mathbf{A}_1)$. For an identity $id \in \{0,1\}^*$, let

$$\mathbf{F}(id) = [\mathbf{A}_0 | \mathbf{A}_1 + H(id) \cdot \mathbf{B}] \in \mathbb{Z}_q^{2\times 2\ell},$$

where $H : \{0,1\}^* \to \mathbb{Z}_q$ is a collision-resistant hash function.

– Extract: on input id, return $sk_{id} = g^{\mathbf{v}}$ where $\mathbf{v} \in \mathbb{Z}_q^{2\ell\times 1}$ is a random vector such that

$$\mathbf{F}(id) \cdot \mathbf{v} = \mathbf{D}. \tag{1}$$

It is easy to generate such $g^{\mathbf{v}}$ from msk using linear algebra. See Appendix A for details.

– Enc: on input id and $M \in \mathbb{G}_T$, take $\mathbf{z} \xleftarrow{\$} \mathbb{Z}_q^{1\times 2}$ and compute

$$C = g^{\mathbf{z}\cdot\mathbf{F}(id)},\ E = \hat{e}(g,g)^{\mathbf{z}\cdot\mathbf{D}} \cdot M,$$

and return (C, E) as the ciphertext.

– Dec: On input $sk_{id} = g^{\mathbf{v}}$ and $C = g^{\mathbf{c}}$, compute

$$K = \hat{e}(g,g)^{\mathbf{c}\cdot\mathbf{v}} \text{ and } M = EK^{-1}$$

using the bi-linearity of $\hat{e}$, and return M. Note that if $\mathbf{c} = \mathbf{z}\mathbf{F}(id)$ then $\mathbf{c}\mathbf{v} = \mathbf{z}(\mathbf{F}(id)\mathbf{v}) = \mathbf{z}\mathbf{D}$, and the completeness follows.

Trapdoor Instead of generating $\mathbf{A}_1$ as above, suppose that

$$\mathbf{A}_1 = \mathbf{A}_0\mathbf{R}^* - H(id^*)\mathbf{B}$$

for $\mathbf{R}^* \xleftarrow{\$} \mathbb{Z}_q^{\ell\times\ell}$ and the target identity id^*. Since $\mathbf{R}^*$ is freshly random, $\mathbf{A}_1$ is correctly distributed. The matrix $\mathbf{R}^*$ will be the trapdoor utilized in security proofs. Then from pp and $\mathbf{R}^*$, we can compute $sk_{id} = g^{\mathbf{v}}$ for any identity id ($\neq id^*$) as follows.

1. First randomly choose $\mathbf{w} \in \mathbb{Z}_q^{\ell\times 1}$.
2. Next consider a random $\mathbf{x} \in \mathbb{Z}_q^{\ell\times 1}$ such that

$$(H(id) - H(id^*))\mathbf{B}\mathbf{x} = -\mathbf{A}_0\mathbf{w} + \mathbf{D}. \tag{2}$$

It is easy to compute $g^{\mathbf{x}}$ from $\mathbf{B}, g^{\mathbf{A}_0}, g^{\mathbf{D}}$ given in pp.

3. Let

$$\mathbf{v} = \begin{bmatrix} \mathbf{w} - \mathbf{R}^*\mathbf{x} \\ \mathbf{x} \end{bmatrix}$$

We can compute $g^{\mathbf{v}}$ by using $g^{\mathbf{x}}$. This $\mathbf{v}$ satisfies eq.(1) because

$$\begin{aligned} \mathbf{F}(id)\mathbf{v} &= [\mathbf{A}_0 | \mathbf{A}_0\mathbf{R}^* + (H(id) - H(id^*))\mathbf{B}] \cdot \begin{bmatrix} \mathbf{w} - \mathbf{R}^*\mathbf{x} \\ \mathbf{x} \end{bmatrix} \\ &= \mathbf{A}_0(\mathbf{w} - \mathbf{R}^*\mathbf{x}) + (\mathbf{A}_0\mathbf{R}^* + (H(id) - H(id^*))\mathbf{B})\mathbf{x} \\ &= \mathbf{A}_0\mathbf{w} + (H(id) - H(id^*))\mathbf{B}\mathbf{x} \\ &= \mathbf{D}. \end{aligned}$$

We show that the above $\mathbf{v}$ is correctly distributed. The solution space of eq.(1) has dimension $2\ell - 2$. On the other hand, $\mathbf{w}$ is chosen from a space of dimension ℓ, and the solution of eq.(2) has freedom $\ell - 2$ since $\mathbf{B} \in \mathbb{Z}_q^{2\times\ell}$. Hence the set of the above $\mathbf{v}$ is equal to the solution space of eq.(1), since $\ell + (\ell - 2) = 2\ell - 2$. The use of trapdoor is similar to [1] in lattice setting.

Theorem 2 *Under the DLIN assumption, the IBE scheme is IND-sID-CPA-secure, leakage resilient with rate* $1 - \frac{3}{2\ell} - \frac{\eta}{\ell|q|}$ *for* η*-bit security. The private key and ciphertext overhead are of* 2ℓ *group elements.*

When $\ell = 3$*, the private key and ciphertext overhead are of* 6 *group elements, with leakage rate* $1/2 - o(1)$*.*

Proof. Let $\mathbf{Game}_0$ be the real attack game against the IBE scheme, and $\mathbf{Game}_1$ be the same as $\mathbf{Game}_0$ except that C^* in the challenge ciphertext is randomly chosen. We first show that the two games are indistinguishable under the DLIN assumption, whose formulation using matrices is in Sect.2.

We will temporarily ignore leakage queries. Given an adversary $\mathcal{A}$ against the IBE scheme, we build $\mathcal{B}$ with input $g^{\mathbf{A}}$ telling whether random $\mathbf{A} \in \mathbb{Z}_q^{3\times\ell}$ is of rank 2 or 3.

After $\mathcal{A}$ announces the target id^*, $\mathcal{B}$ sets up the public parameter $pp = (g^{\mathbf{A}_0}, g^{\mathbf{A}_1}, \mathbf{B}, g^{\mathbf{D}})$ as follows:

- $g^{\mathbf{A}_0}$ is the first two rows of $g^{\mathbf{A}}$. Namely, $\mathbf{A}_0 \in \mathbb{Z}_q^{2\times\ell}$ consists of the two rows of $\mathbf{A}$.
- $\mathcal{B}$ chooses $\mathbf{B} \xleftarrow{\$} \mathbb{Z}_q^{2\times\ell}$ and $\mathbf{R}^* \xleftarrow{\$} \mathbb{Z}_q^{\ell\times\ell}$, and sets $\mathbf{A}_1 = \mathbf{A}_0\mathbf{R}^* - H(id^*)\mathbf{B}$. Certainly $\mathcal{B}$ can compute $g^{\mathbf{A}_1}$ from $g^{\mathbf{A}_0}$. Note that by the above,

$$\begin{aligned} \mathbf{F}(id) &= [\mathbf{A}_0 | \mathbf{A}_1 + H(id)\mathbf{B}] = [\mathbf{A}_0 | \mathbf{A}_0\mathbf{R}^* + (H(id) - H(id^*))\mathbf{B}] \\ \mathbf{F}(id^*) &= [\mathbf{A}_0 | \mathbf{A}_0\mathbf{R}^*]. \end{aligned}$$

- $\mathcal{B}$ chooses $\mathbf{v}^* \xleftarrow{\$} \mathbb{Z}_q^{2\ell\times 1}$ and sets

$$\mathbf{D} = \mathbf{F}(id^*) \cdot \mathbf{v}^* = [\mathbf{A}_0 | \mathbf{A}_0\mathbf{R}^*] \cdot \mathbf{v}^*$$

so that $\mathbf{D} \in \mathbb{Z}_q^{2\times 1}$ is uniformly distributed, and $\mathcal{B}$ can compute $g^{\mathbf{D}}$ from $g^{\mathbf{A}_0}$.

$\mathcal{B}$ simulates $\mathcal{A}$ as follows.

- On extract query $id \neq id^*$, $\mathcal{B}$ computes and returns $g^{\mathbf{v}}$ as shown in the trapdoor above.
- On challenge query (M_0, M_1), denote $\mathbf{y}$ the third row of $\mathbf{A}$, let $b \xleftarrow{\$} \{0, 1\}$, and return

$$(C^*, E^*) = \left(g^{[\mathbf{y}|\mathbf{y}\mathbf{R}^*]}, \hat{e}(g, g)^{[\mathbf{y}|\mathbf{y}\mathbf{R}^*]\mathbf{v}^*} M_b \right).$$

- Finally, $\mathcal{A}$ outputs b'. If $b' = b$, $\mathcal{B}$ bets that $\mathbf{A}$ is of rank 2. Otherwise, it guesses $\mathbf{A}$ is of rank 3.

We will show that (C^*, E^*) is the ciphertext in $\mathbf{Game}_0$ if $\mathsf{rank}(\mathbf{A}) = 2$; while it is in $\mathbf{Game}_1$ if $\mathsf{rank}(\mathbf{A}) = 3$.

– Suppose that $\mathsf{rank}(\mathbf{A}) = 2$. Then $\mathbf{y}$ is a linear combination of the first two rows of $\mathbf{A}_0$, namely $\mathbf{y} = \mathbf{z}^*\mathbf{A}_0$ for some $\mathbf{z}^* \in \mathbb{Z}_q^{1\times 2}$. Therefore

$$[\mathbf{y}|\mathbf{y}\mathbf{R}^*] = [\mathbf{z}^*\mathbf{A}_0|\mathbf{z}^*\mathbf{A}_0\mathbf{R}^*] = \mathbf{z}^*[\mathbf{A}_0|\mathbf{A}_0\mathbf{R}^*] = \mathbf{z}^* \cdot \mathbf{F}(id^*),$$

showing that (C^*, E^*) is the ciphertext in $\mathbf{Game}_0$.

– Suppose that $\mathsf{rank}(\mathbf{A}) = 3$. Then $\mathbf{y}$ is random in $\mathbb{Z}_q^{1\times\ell}$. It suffices to prove that

$$\mathbf{d} = \mathbf{y}\mathbf{R}^*$$

is also random in $\mathbb{Z}_q^{1\times\ell}$ even given $\mathbf{A}_0$, $\mathbf{U} = \mathbf{A}_0\mathbf{R}^*$, $\mathbf{y}$.
It is easy to see that

$$\mathbf{A} \cdot \mathbf{R}^* = \begin{bmatrix} \mathbf{U} \\ \mathbf{d} \end{bmatrix}.$$

Therefore, for any $\mathbf{d}$, there exists a unique $\mathbf{R}^*$ such that the above equation holds because $\mathbf{A}$ is of full rank (with all but negligible probability). This means that $\mathbf{d}$ is random since $\mathbf{R}^*$ is random and hence C^* is random as expected.

Thus $\mathbf{Game}_0$ and $\mathbf{Game}_1$ are indistinguishable under the DLIN assumption. Let p_i be the success probability $\Pr[b' = b]$ of the adversary $\mathcal{A}$ in $\mathbf{Game}_i$ for $i = 0, 1$, so that $|p_0 - p_1|$ is computationally negligible. We will show that $p_1 = 1/2$ to finish the proof.

First C^* is now written as $C^* = g^{\mathbf{c}^*}$ for some $\mathbf{c}^* \in \mathbb{Z}_q^{1\times 2\ell}$. Then

$$E^* = \hat{e}(g, g)^{\mathbf{c}^*\cdot\mathbf{v}^*} M_b.$$

Let

$$\alpha = \mathbf{c}^* \cdot \mathbf{v}^*,$$

and remember that

$$\mathbf{D} = \mathbf{F}(id^*) \cdot \mathbf{v}^* \tag{3}$$

we obtain

$$\begin{bmatrix} \alpha \\ \mathbf{D} \end{bmatrix} = \begin{bmatrix} \mathbf{c}^* \\ \mathbf{F}(id^*) \end{bmatrix} \mathbf{v}^*.$$

In $\mathbf{Game}_1$, $\mathbf{c}^*$ is random because C^* is random. Hence $\mathbf{c}^*$ is linearly independent of the two rows of $\mathbf{F}(id^*)$ with overwhelming probability. This means that α is random even given $\mathbf{c}^*, \mathbf{D}, \mathbf{F}(id^*)$ because $\mathbf{v}^*$ is random. Thus $E^* = \hat{e}(g, g)^\alpha M_b$ is random, and hence $p_1 = 1/2$ as claimed. Therefore the advantage of $\mathcal{A}$ against the IBE scheme

$$\left| p_0 - \frac{1}{2} \right| = |p_0 - p_1|$$

is negligible under the DLIN assumption.

Let us now consider leakage resilience. Consider the leakage function $f : \mathbb{Z}_q^{2\ell} \to Z$ encoding of all leakage queries f_i, for some set Z (whose order is decided below). We want to prove that the distributions

$$\Big(\mathbf{c}^*, \mathbf{c}^*\mathbf{v}^*, f(\mathbf{v}^*)\Big) \text{ and } \Big(\mathbf{c}^*, \mathsf{U}_{\mathbb{Z}_q}, f(\mathbf{v}^*)\Big)$$

are statistically indistinguishable, which means $\alpha = \mathbf{c}^*\mathbf{v}^*$ is randomly distributed conditioned on $\mathbf{c}^* = \log_g C^*$ and the leakage $f(\mathbf{v}^*)$.

Now re-consider the games, now with leakage queries. Since the simulator $\mathcal{B}$ for the DLIN assumption can generate $\mathbf{v}^*$, $\mathbf{Game}_0$ and $\mathbf{Game}_1$ are still indistinguishable even given $f(\mathbf{v}^*)$. Furthermore, in $\mathbf{Game}_1$, $\mathbf{c}^*$ is random over $\mathbb{Z}_q^{1\times 2\ell}$. Let $h_{\mathbf{c}^*}(\mathbf{r}) = \mathbf{c}^*\mathbf{r}$ maps $\mathbf{r} \in \mathbb{Z}_q^{2\ell\times 1}$ to $\mathbb{Z}_q$. Since $\Pr_{\mathbf{c}^*}[h_{\mathbf{c}^*}(\mathbf{r}) = h_{\mathbf{c}^*}(\mathbf{r}')] = 1/q$ for $\mathbf{r} \neq \mathbf{r}'$, the function $h_{\mathbf{c}^*}$ is universal. Applying Lemma 1, the statistical distance of the above distributions is at most

$$\frac{1}{2}\sqrt{\gamma(\mathbf{v}^*) \cdot q \cdot |Z|}$$

in which $\gamma(\mathbf{v}^*) = \max_{\mathbf{u}\in\mathbb{Z}_q^{2\ell}} \Pr[\mathbf{v}^* = \mathbf{u}]$.

Now that $\mathbf{v}^*$ is random satisfying $\mathbf{F}(id^*)\mathbf{v}^* = \mathbf{D}$, its freedom is $2\ell - 2$. Therefore $\gamma(\mathbf{v}^*) = q^{2-2\ell}$ so that we can choose $|Z| = q^{2\ell-3}2^{-2\eta}$ for η-bit security, namely the leakage on $\mathbf{v}^*$ can be of $(2\ell-3)|q| - 2\eta$ bits. Therefore the leakage rate is

$$\frac{(2\ell-3)|q| - 2\eta}{2\ell|q|} = 1 - \frac{3}{2\ell} - \frac{\eta}{\ell|q|} = 1 - o(1)$$

as claimed. □

Remark. Above we neglect a technical point in estimating the leakage rate. Let G be an elliptic curve over $\mathbb{Z}_p$ for some prime p, so each element in G can be represented in about $|p|$ bits. Thus private key size is $|g^{\mathbf{v}^*}| \approx 2\ell|p|$ bits. Now, the rate is more precisely

$$\frac{|\mathsf{leak}(g^{\mathbf{v}^*})|}{|g^{\mathbf{v}^*}|} \approx \frac{(2\ell-3)|q| - 2\eta}{2\ell|p|}$$

so that to claim the rate $1 - o(1)$, we need $|q|/|p| \approx 1$. This requirement is satisfied by practical choices of q and p (e.g., [10, Table 1]).

This remark applies as well for estimating the leakage rate in following sections.

3.2 Fully secure scheme under DLIN

For an identity id expressed as a bit sequence $id = id[1]||\cdots||id[m]$, consider the KEM in the previous section, yet employing the matrix

$$\mathbf{F}(id) = \left[\mathbf{A}_0 \middle| \mathbf{A}'_0 + \sum_{i=1}^{m} id[i]\mathbf{A}_i\right] \in \mathbb{Z}_q^{2\times 2\ell},$$

where $\mathbf{A}_0, \mathbf{A}_1, \ldots, \mathbf{A}_m, \mathbf{A}'_0 \in \mathbb{Z}_q^{2\times\ell}$ are random matrices employed as the master secret key. In the public parameters, the matrices are given in the exponents.

Theorem 3 *Employing the above $\mathbf{F}(id)$, the IBE scheme in Section 3.1 is IND-ID-CPA-secure under the DLIN assumption, and leakage resilient with rate $1 - \frac{3}{2\ell} - \frac{\eta}{\ell|q|}$ for η-bit security. The private key and ciphertext overhead are of 2ℓ group elements.*

When $\ell = 3$, the private key and ciphertext overhead are of 6 group elements, with leakage rate $1/2 - o(1)$.

In the security reduction, we use the artificial abort technique of Waters [25]. (Note that one may also use the technique in [7] to improve the concrete security. Then the artificial abort technique is not needed either.) We construct a simulator $\mathcal{B}$ as follows. $\mathcal{B}$ first sets $J = 4Q$, where Q is the total number of (extract, leakage, reveal) queries of the adversary. $\mathcal{B}$ chooses $k \xleftarrow{\$} \{0, \ldots, m\}$ and $h_i \xleftarrow{\$} \mathbb{Z}_J$ for $i = 0, 1, \ldots, m$. $\mathcal{B}$ then constructs the matrices $\mathbf{A}'_0$ and each $\mathbf{A}_i$ (excluding $\mathbf{A}_0$) as

$$\mathbf{A}'_0 = \mathbf{A}_0\mathbf{R}_0 + (q - kJ + h_0)\mathbf{C}$$
$$\mathbf{A}_i = \mathbf{A}_0\mathbf{R}_i + h_i\mathbf{C}$$

where $\mathbf{C} \leftarrow \mathbb{Z}_q^{2\times\ell}$, and $\mathbf{R}_i \leftarrow \mathbb{Z}_q^{\ell\times\ell}$. Then

$$\mathbf{F}(id) = \left[\mathbf{A}_0 \middle| \mathbf{A}_0(\mathbf{R}_0 + \sum_{i=1}^{m} id[i]\mathbf{R}_i) + (q - kJ + h_0 + \sum_{i=1}^{m} id[i]h_i)\mathbf{C}\right]$$

Let

$$\alpha(id) = q - kJ + h_0 + \sum_{i=1}^{m} id[i]h_i.$$

$\mathcal{B}$ can succeed if

$$\alpha(id^*) = 0 \bmod q$$

and for all extract query $id \neq id^*$,

$$\alpha(id) \neq 0 \bmod q.$$

This probability λ is lower bounded by

$$\lambda \geq \frac{1}{(m+1)J}\left(1 - 2\frac{Q}{J}\right)$$

similarly to [25, Sect.5.2, eq.(1k)]. For completeness, we recall the estimation in Appendix B. With the probability λ,

$$\mathbf{F}(id^*) = \left[\mathbf{A}_0 \middle| \mathbf{A}_0(\mathbf{R}_0 + \sum_{i=1}^{m} id^*[i]\mathbf{R}_i)\right],$$

so that the proof proceeds identically with that of Theorem 2 just by letting

$$\mathbf{R}^* = \mathbf{R}_0 + \sum_{i=1}^{m} id^*[i]\mathbf{R}_i$$

except for that we use the artificial abort, and the following.

$\mathcal{A}$ does not announce the target id^* at the beginning of the attack game in the model of full security. Hence $\mathcal{B}$ cannot compute $\mathbf{v}^*$ nor $g^{\mathbf{D}}$ as in the proof of Theorem 2.

1. Therefore $\mathcal{B}$ first chooses $\mathbf{E} \in \mathbb{Z}_q^{\ell \times 1}$ randomly and consider $\mathbf{D} \in \mathbb{Z}_q^{2\times 1}$ such that

   $$\mathbf{D} = \mathbf{A}_0\mathbf{E}.$$

   $\mathcal{B}$ computes $g^{\mathbf{D}}$ from $g^{\mathbf{A}_0}$ and $\mathbf{E}$. Moreover, given $\mathbf{D}$ and for $\mathbf{E} = (\mathbf{E}[1], \ldots, \mathbf{E}[\ell])^T$, we can let the components $\mathbf{E}[3], \ldots, \mathbf{E}[\ell]$ free in $\mathbb{Z}_q$ since $\mathbf{A}_0 \in \mathbb{Z}_q^{2\times\ell}$ is of rank 2.
2. The simulation of queries depends on $\alpha(id)$: There are two cases for each query id. Firstly, if $\alpha(id) \neq 0$, the corresponding $\mathbf{v}$ is set to

   $$\mathbf{v} = \begin{bmatrix} \mathbf{w} - (\mathbf{R}_0 + \sum_{i=1}^{m} id[i]\mathbf{R}_i)\mathbf{x} \\ \mathbf{x} \end{bmatrix}$$

   in which $\mathbf{w}$ is random and $\mathbf{x}$ satisfies $\alpha(id)\mathbf{C}\mathbf{x} = \mathbf{D} - \mathbf{A}_0\mathbf{w}$. Thus $sk_{id} = g^{\mathbf{v}}$ can be computed, and hence extraction, leakage, and reveal queries can be simulated.
   In the second case of target identity $id = id^*$, namely $\alpha(id^*) = 0$, $\mathcal{B}$ can again compute private key $sk_{id^*} = g^{\mathbf{v}^*}$ by solving $\mathbf{v}^* = (\mathbf{v}^*[1], \ldots, \mathbf{v}^*[2\ell])^T$ satisfying

   $$\left[\mathbf{I}_\ell \;\middle|\; \mathbf{R}^*\right] \cdot \mathbf{v}^* = \mathbf{E}$$

   where $\mathbf{I}_\ell \in \mathbb{Z}_q^{\ell\times\ell}$ is the identity matrix. It is easy to see that $g^{\mathbf{v}^*}$ is the private key for id^* by multiplying $\mathbf{A}_0$ from the left to both hand sides of the above equation. From that equation, we now have

   $$\begin{bmatrix} \mathbf{v}^*[1] \\ \vdots \\ \mathbf{v}^*[\ell] \end{bmatrix} = \begin{bmatrix} \mathbf{E}[1] \\ \vdots \\ \mathbf{E}[\ell] \end{bmatrix} - \mathbf{R}^* \begin{bmatrix} \mathbf{v}^*[\ell+1] \\ \vdots \\ \mathbf{v}^*[2\ell] \end{bmatrix}.$$

   Since $\mathbf{E}[3], \ldots, \mathbf{E}[\ell], \mathbf{v}^*[\ell+1], \ldots, \mathbf{v}^*[2\ell]$ can be independently random in $\mathbb{Z}_q$, there are $q^{(\ell-2)+\ell}$ choices for $\mathbf{v}^*$, so that it is from a space of dimension $2\ell - 2$ as expected. The leakage rate for η-bit security

   $$1 - \frac{3}{2\ell} - \frac{\eta}{\ell|q|}$$

   is computed exactly as in the selective case.

4 Proposed IPE under DLIN

In this section we design the first leakage resilient IPE scheme under the DLIN assumption with leakage rate $1 - o(1)$. Several techniques in previous sections are re-utilized here.

Below $id = (id_1, \ldots, id_n) \in \mathbb{Z}_q^n$. For $u = (u_1, \ldots, u_n) \in \mathbb{Z}_q^n$, decryption will work correctly if

$$\langle id, u \rangle = \sum_{i=1}^{n} id_i u_i = 0 \in \mathbb{Z}_q.$$

The scheme is as follows.

- Setup: Take $\mathbf{A}_i, \mathbf{S} \xleftarrow{\$} \mathbb{Z}_q^{2\times \ell}$ and $\mathbf{D} \xleftarrow{\$} \mathbb{Z}_q^{2\times 1}$, let

$$msk = (\mathbf{A}_0, \ldots, \mathbf{A}_n),\ mpk = (g^{\mathbf{A}_0}, \ldots, g^{\mathbf{A}_n}, g^{\mathbf{D}}, \mathbf{S}).$$

- $\mathsf{Extract}_{msk}(id)$: Return $g^{\mathbf{v}} \in \mathbb{G}^{2\ell \times 1}$ where

$$\mathbf{F}(id) \cdot \mathbf{v} = \left[\mathbf{A}_0 \middle| \sum_{i=1}^{n} id_i \mathbf{A}_i \right] \cdot \mathbf{v} = \mathbf{D}.$$

- $\mathsf{Enc}(u, M \in \mathbb{G}_T)$: Take $\mathbf{z} \xleftarrow{\$} \mathbb{Z}_q^{1\times 2}$, return

$$C = g^{\mathbf{z}[\mathbf{A}_0 | \mathbf{A}_1 + u_1 \mathbf{S} | \cdots | \mathbf{A}_n + u_n \mathbf{S}]} \text{ and } E = e(g,g)^{\mathbf{z}\cdot\mathbf{D}} M.$$

- $\mathsf{Dec}_{g^{\mathbf{v}}}(id, C, E)$: From

$$C = g^{[\mathbf{y}|\mathbf{y}_1|\cdots|\mathbf{y}_n]}$$

compute

$$\prod_{i=1}^{n} (g^{\mathbf{y}_i})^{id_i} = g^{\sum_{i=1}^{n} id_i \mathbf{y}_i},$$

and hence obtain $g^{[\mathbf{y}|\sum_{i=1}^{n} id_i \mathbf{y}_i]}$. Pair that with the private key $g^{\mathbf{v}}$, obtaining

$$F = e(g,g)^{[\mathbf{y}|\sum_{i=1}^{n} id_i \mathbf{y}_i]\cdot \mathbf{v}} \in \mathbb{G}_T$$

and finally compute the message $m = E \cdot F^{-1}$.

Correctness. Following directly from below equations

$$\begin{aligned}
\left[\mathbf{y} | \sum_{i=1}^{n} id_i \mathbf{y}_i \right] &= \left[\mathbf{z}\mathbf{A}_0 | \sum_{i=1}^{n} id_i \mathbf{z}(\mathbf{A}_i + u_i \mathbf{S}) \right] \\
&= \left[\mathbf{z}\mathbf{A}_0 | \mathbf{z} \sum_{i=1}^{n} id_i \mathbf{A}_i + \langle id, u \rangle \mathbf{z}\mathbf{S} \right] \\
&= \left[\mathbf{z}\mathbf{A}_0 | \mathbf{z} \sum_{i=1}^{n} id_i \mathbf{A}_i \right] = \mathbf{z}\mathbf{F}(id).
\end{aligned}$$

Theorem 4 *The above IPE scheme is leakage resilient under the DLIN assumption with leakage rate* $1 - \frac{3}{2\ell} - \frac{\eta}{\ell |q|}$ *for* η*-bit security.*

Proof. We will consider the following games:

- $\mathbf{Game}_0$: This is the original attack game.
- $\mathbf{Game}_1$: In this game, $\log_g C^* = [\mathbf{y}|\mathbf{y}_1| \cdots |\mathbf{y}_n]$ is chosen randomly.

The road map is as follows. Temporarily ignoring leakage queries, we will prove that the games are indistinguishable under the DLIN assumption (in Sect.2). In addition, we prove in $\mathbf{Game}_1$ that E^* and C^* do not contain any information on the hidden challenge bit b. We will deal with leakage queries at the end of the proof.

Consider an adversary $\mathcal{A}$ against the scheme which can tell apart $\mathbf{Game}_0$ and $\mathbf{Game}_1$, we build $\mathcal{B}$ against DLIN. $\mathcal{A}$ gets $g^{\mathbf{A}}$ as input for $\mathbf{A} \in \mathbb{Z}_q^{3\times\ell}$, and will decide whether $\mathbf{A}$ is of rank 2 or 3.

At first, $\mathcal{A}$ outputs $u^{(0)}, u^{(1)} \in \mathbb{Z}_q^n$. $\mathcal{B}$ considers $g^{\mathbf{A}_0}$ as the first two rows of $g^{\mathbf{A}}$, and $g^{\mathbf{y}}$ as the third one. $\mathcal{B}$ lets for $1 \le i \le n$,

$$\mathbf{A}_i = \mathbf{A}_0\mathbf{R}_i^* - u_i^{(b)}\mathbf{S},$$

where $b \xleftarrow{\$} \{0,1\}, \mathbf{R}_i^* \xleftarrow{\$} \mathbb{Z}_q^{\ell\times\ell}, \mathbf{S} \xleftarrow{\$} \mathbb{Z}_q^{2\times\ell}$ chosen by $\mathcal{B}$, and hence

$$\mathbf{F}(id) = \left[\mathbf{A}_0 \middle| \sum_{i=1}^n id_i\mathbf{A}_i\right] = \left[\mathbf{A}_0 \middle| \mathbf{A}_0\sum_{i=1}^n id_i\mathbf{R}_i^* - \langle id, u^{(b)}\rangle\mathbf{S}\right].$$

Let $\mathbf{D} = \mathbf{A}_0\mathbf{E}$ where $\mathbf{E} \xleftarrow{\$} \mathbb{Z}_q^{\ell\times 1}$ by $\mathcal{B}$, so $g^{\mathbf{D}}$ can be computed from $g^{\mathbf{A}_0}$.
Then $\mathcal{B}$ feeds $mpk = (g^{\mathbf{A}_0}, \ldots, g^{\mathbf{A}_n}, g^{\mathbf{D}}, \mathbf{S})$ to $\mathcal{A}$, simulating its queries as follows.

- **Extract query** $id \in \mathbb{Z}_q^n$ **where** $\alpha = \langle id, u^{(b)}\rangle \neq 0$**:** $\mathcal{B}$ needs to return $g^{\mathbf{v}}$ where

$$\mathbf{F}(id)\mathbf{v} = \left[\mathbf{A}_0 \middle| \mathbf{A}_0\sum_{i=1}^n id_i\mathbf{R}_i^* - \alpha\mathbf{S}\right]\cdot\mathbf{v} = \mathbf{D}\ (= \mathbf{A}_0\mathbf{E}).$$

  Since $\alpha \neq 0$, let $\mathbf{w} \xleftarrow{\$} \mathbb{Z}_q^{\ell\times 1}$, and set

$$\mathbf{v} = \begin{bmatrix}\mathbf{w} - (\sum_{i=1}^n id_i\mathbf{R}_i^*)\mathbf{x}\\ \mathbf{x}\end{bmatrix}$$

  where $\mathbf{x} \in \mathbb{Z}_q^{\ell\times 1}$ satisfies

$$\alpha\mathbf{S}\mathbf{x} = \mathbf{A}_0\mathbf{w} - \mathbf{D},$$

  so that $g^{\mathbf{x}}$, and hence $g^{\mathbf{v}}$ can be computed by $\mathcal{B}$.
- **The target key:** Note that if $\alpha = 0$, it is sufficient that $\mathbf{v}$ satisfies

$$\left[\mathbf{I}_\ell \middle| \sum_{i=1}^n id_i\mathbf{R}_i^*\right]\cdot\mathbf{v} = \mathbf{E},$$

  where $\mathbf{I}_\ell$ is the identity matrix of rank ℓ. That $\mathbf{v}$ is easily computed. In particular, for $id^* \in \mathbb{Z}_q^n$ satisfying $\langle id^*, u^{(b)}\rangle = 0$, the corresponding $\mathbf{v}^*$ can be computed by $\mathcal{B}$. This fact will be used later.
- **Challenge query** $M^{(0)}, M^{(1)}$: $\mathcal{B}$ simply returns

$$C^* = g^{[\mathbf{y}|\mathbf{y}_1|\cdots|\mathbf{y}_n]} \text{ and } E^* = e(g,g)^{[\mathbf{y}|\sum_{i=1}^n id_i^*\mathbf{y}_i]\cdot\mathbf{v}^*}\cdot M^{(b)}$$

  where $\mathbf{y}_i = \mathbf{y}\mathbf{R}_i^*$ for $1 \le i \le n$.
- Finally $\mathcal{A}$ returns b'. If $b' = b$, $\mathcal{B}$ bets $\mathbf{A}$ is of rank 2; otherwise bets $\mathbf{A}$ is of rank 3.

We will show that (C^*, E^*) is a legitimate ciphertext of $u^{(b)}, M^{(b)}$ if $\mathbf{A}$ is of rank 2, while $\log_g C^* = [\mathbf{y}|\mathbf{y}_1|\cdots|\mathbf{y}_n]$ is random if $\mathbf{A}$ is of rank 3. Let us consider the following cases.

$\mathbf{A}$ is of rank 2: We have $\mathbf{y} = \mathbf{z}^*\mathbf{A}_0$ for some random $\mathbf{z}^*$. Therefore, as expected,

$$\begin{aligned} C^* = g^{[\mathbf{z}^*\mathbf{A}_0|\mathbf{z}^*\mathbf{A}_0\mathbf{R}_1^*|\cdots|\mathbf{z}^*\mathbf{A}_0\mathbf{R}_n^*]} &= g^{\mathbf{z}^*[\mathbf{A}_0|\mathbf{A}_0\mathbf{R}_1^*|\cdots|\mathbf{A}_0\mathbf{R}_n^*]} \\ &= g^{\mathbf{z}^*[\mathbf{A}_0|\mathbf{A}_1+u_1^{(b)}\mathbf{S}|\cdots|\mathbf{A}_n+u_n^{(b)}\mathbf{S}]}. \end{aligned}$$

A is of rank 3: This means $\mathbf{y}$ is random in $\mathbb{Z}_q^{1\times\ell}$. We need to show that $\mathbf{y}_i = \mathbf{y}\mathbf{R}_i^*$ is random for all $1 \le i \le n$, even given $\mathbf{A}_0\mathbf{R}_i^*$ (in $\mathbf{A}_i$). This is justified since

$$\begin{bmatrix} \mathbf{A}_0\mathbf{R}_i^* \\ \mathbf{y}_i \end{bmatrix} = \begin{bmatrix} \mathbf{A}_0 \\ \mathbf{y} \end{bmatrix} \cdot \mathbf{R}_i^*$$

in which $\mathbf{A} = \begin{bmatrix} \mathbf{A}_0 \\ \mathbf{y} \end{bmatrix}$ is of full rank. Since $\mathbf{R}_i^*$ is random, so is $\mathbf{y}_i = \mathbf{y}\mathbf{R}_i^*$ as required.

The above arguments ensure that $\mathbf{Game}_0$ and $\mathbf{Game}_1$ are indistinguishable under the DLIN assumption. Now we move into $\mathbf{Game}_1$ in which, for $\mathbf{y}, \mathbf{y}_1, \ldots, \mathbf{y}_n \xleftarrow{\$} \mathbb{Z}_q^{1\times\ell}$,

$$C^* = g^{[\mathbf{y}|\mathbf{y}_1|\cdots|\mathbf{y}_n]} \text{ and } E^* = e(g,g)^{[\mathbf{y}|\sum_{i=1}^n id_i^*\mathbf{y}_i]\cdot\mathbf{v}^*} \cdot M^{(b)}.$$

We will show

$$e^* = \left[\mathbf{y}\middle|\sum_{i=1}^n id_i^*\mathbf{y}_i\right] \cdot \mathbf{v}^*$$

is randomly distributed in $\mathbb{Z}_q$. For that, consider the equation

$$\begin{bmatrix} e^* \\ \mathbf{D} \end{bmatrix} = \begin{bmatrix} \mathbf{y}|\sum_{i=1}^n id_i^*\mathbf{y}_i \\ \mathbf{F}(id^*) \end{bmatrix} \cdot \mathbf{v}^*,$$

and note that $[\mathbf{y}|\sum_{i=1}^n id_i^*\mathbf{y}_i]$ is independent with the rows of $\mathbf{F}(id^*)$ (with all but negligible probability). Thus e^* is random even conditioned on $\mathbf{D}$. Therefore, both C^* and E^* are truly random in $\mathbf{Game}_1$, and hence $\Pr[b' = b] = 1/2$ in this game. Thus $|\Pr[b' = b] - 1/2|$ in $\mathbf{Game}_0$ is negligible under the DLIN assumption.

Up to now, we did not consider leakage queries. Let us now examine them. Consider the leakage function $f : \mathbb{Z}_q^{2\ell} \to Z$ encoding of all leakage queries f_i, for some set Z (whose order is decided below). We want to prove that the distributions

$$\Big(\mathbf{c}^*, \mathbf{c}^*\mathbf{v}^*, f(\mathbf{v}^*)\Big) \text{ and } \Big(\mathbf{c}^*, \mathsf{U}_{\mathbb{Z}_q}, f(\mathbf{v}^*)\Big),$$

for $\mathbf{c}^* = [\mathbf{y}|\sum_{i=1}^n id_i^*\mathbf{y}_i]$, are statistically indistinguishable, which means $\mathbf{c}^*\mathbf{v}^*$ is randomly distributed conditioned on $\mathbf{c}^*$ and the leakage $f(\mathbf{v}^*)$. Thus $\hat{e}(g,g)^{\mathbf{c}^*\cdot\mathbf{v}^*}$ and hence E^* are also randomly distributed.

Now re-consider the games. Since the simulator $\mathcal{B}$ for the DLIN assumption can generate $\mathbf{v}^*$, $\mathbf{Game}_0$ and $\mathbf{Game}_1$ are still indistinguishable even given $f(\mathbf{v}^*)$. Furthermore, in $\mathbf{Game}_1$, $\mathbf{c}^*$ is random over $\mathbb{Z}_q^{1\times 2\ell}$. Let $h_{\mathbf{c}^*}(\mathbf{r}) = \mathbf{c}^*\mathbf{r}$ maps $\mathbf{r} \in \mathbb{Z}_q^{2\ell\times 1}$ to $\mathbb{Z}_q$. Since $\Pr_{\mathbf{c}^*}[h_{\mathbf{c}^*}(\mathbf{r}) = h_{\mathbf{c}^*}(\mathbf{r}')] = 1/q$ for $\mathbf{r} \neq \mathbf{r}'$, the function $h_{\mathbf{c}^*}$ is universal. Applying the leftover hash lemma (Lemma 1), the statistical distance of the above distributions is at most

$$\frac{1}{2}\sqrt{\gamma(\mathbf{v}^*) \cdot q \cdot |Z|}$$

in which $\gamma(\mathbf{v}^*) = \max_{\mathbf{u}\in\mathbb{Z}_q^{2\ell}} \Pr[\mathbf{v}^* = \mathbf{u}]$.

Recall that $\mathbf{v}^*$ is random satisfying $\mathbf{F}(id^*)\mathbf{v}^* = \mathbf{D}$. Since $\mathbf{F}(id^*) \in \mathbb{Z}_q^{2\times 2\ell}$, the freedom of $\mathbf{v}^*$ is $2\ell - 2$. Therefore $\gamma(\mathbf{v}^*) = q^{2-2\ell}$ so that we can choose $|Z| = q^{2\ell-3}2^{-2\eta}$ for η-bit security, namely the leakage on $\mathbf{v}^*$ can be of $(2\ell-3)|q| - 2\eta$ bits. In turn,

$$\frac{(2\ell-3)|q| - 2\eta}{2\ell|q|} = 1 - \frac{3}{2\ell} - \frac{\eta}{\ell|q|} = 1 - o(1)$$

fraction of the private key $sk_{id^*} = g^{\mathbf{v}^*}$ can be leaked. □

References

1. S. Agrawal, D. Boneh, and X. Boyen. Efficient lattice (H)IBE in the standard model. In Gilbert [14], pages 553–572.
2. S. Agrawal, D. M. Freeman, and V. Vaikuntanathan. Functional encryption for inner product predicates from learning with errors. Cryptology ePrint Archive, Report 2011/410, 2011. `http://eprint.iacr.org/`. Accepted to Asiacrypt 2011.
3. A. Akavia, S. Goldwasser, and V. Vaikuntanathan. Simultaneous hardcore bits and cryptography against memory attacks. In O. Reingold, editor, *TCC*, volume 5444 of *Lecture Notes in Computer Science*, pages 474–495. Springer, 2009.
4. J. Alwen, Y. Dodis, M. Naor, G. Segev, S. Walfish, and D. Wichs. Public-key encryption in the bounded-retrieval model. In Gilbert [14], pages 113–134.
5. J. Alwen, Y. Dodis, and D. Wichs. Survey: Leakage resilience and the bounded retrieval model. In K. Kurosawa, editor, *ICITS*, volume 5973 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2009.
6. M. Bellare, E. Kiltz, C. Peikert, and B. Waters. Identity-based (lossy) trapdoor functions and applications. In Pointcheval and Johansson [23], pages 228–245.
7. M. Bellare and T. Ristenpart. Simulation without the artificial abort: Simplified proof and improved concrete security for Waters' IBE scheme. In A. Joux, editor, *EUROCRYPT*, volume 5479 of *Lecture Notes in Computer Science*, pages 407–424. Springer, 2009.
8. M. Bellare, B. Waters, and S. Yilek. Identity-based encryption secure against selective opening attack. In Ishai [15], pages 235–252.
9. D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In M. K. Franklin, editor, *CRYPTO*, volume 3152 of *Lecture Notes in Computer Science*, pages 41–55. Springer, 2004.
10. D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. *J. Cryptology*, 17(4):297–319, 2004.
11. D. Boneh and B. Waters. Conjunctive, subset, and range queries on encrypted data. In S. P. Vadhan, editor, *TCC*, volume 4392 of *Lecture Notes in Computer Science*, pages 535–554. Springer, 2007.
12. Z. Brakerski, Y. T. Kalai, J. Katz, and V. Vaikuntanathan. Overcoming the hole in the bucket: Public-key cryptography resilient to continual memory leakage. In L. Trevisan, editor, *FOCS*, pages 501–510. IEEE Computer Society, 2010. Full version available at `http://eprint.iacr.org/2010/278.pdf`.
13. S. S. M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters. Practical leakage-resilient identity-based encryption from simple assumptions. In E. Al-Shaer, A. D. Keromytis, and V. Shmatikov, editors, *ACM Conference on Computer and Communications Security*, pages 152–161. ACM, 2010.
14. H. Gilbert, editor. *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010. Proceedings*, volume 6110 of *Lecture Notes in Computer Science*. Springer, 2010.
15. Y. Ishai, editor. *Theory of Cryptography - 8th Theory of Cryptography Conference, TCC 2011, Providence, RI, USA, March 28-30, 2011. Proceedings*, volume 6597 of *Lecture Notes in Computer Science*. Springer, 2011.
16. J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In N. P. Smart, editor, *EUROCRYPT*, volume 4965 of *Lecture Notes in Computer Science*, pages 146–162. Springer, 2008.
17. A. B. Lewko. Tools for simulating features of composite order bilinear groups in the prime order setting. In Pointcheval and Johansson [23], pages 318–335.
18. A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In Gilbert [14], pages 62–91.
19. A. B. Lewko, Y. Rouselakis, and B. Waters. Achieving leakage resilience through dual system encryption. In Ishai [15], pages 70–88.
20. M. Naor and G. Segev. Public-key cryptosystems resilient to key leakage. In S. Halevi, editor, *CRYPTO*, volume 5677 of *Lecture Notes in Computer Science*, pages 18–35. Springer, 2009. Full version available at `http://research.microsoft.com/en-us/um/people/gilse/papers/KeyLeakage.pdf`.
21. T. Okamoto and K. Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In T. Rabin, editor, *CRYPTO*, volume 6223 of *Lecture Notes in Computer Science*, pages 191–208. Springer, 2010.
22. T. Okamoto and K. Takashima. Adaptively attribute-hiding (hierarchical) inner product encryption. In Pointcheval and Johansson [23], pages 591–608.
23. D. Pointcheval and T. Johansson, editors. *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, volume 7237 of *Lecture Notes in Computer Science*. Springer, 2012.
24. A. Shamir. Identity-based cryptosystems and signature schemes. In *CRYPTO*, pages 47–53, 1984.
25. B. Waters. Efficient identity-based encryption without random oracles. In R. Cramer, editor, *EUROCRYPT*, volume 3494 of *Lecture Notes in Computer Science*, pages 114–127. Springer, 2005.
26. T. H. Yuen, S. S. M. Chow, Y. Zhang, and S. M. Yiu. Identity-based encryption resilient to continual auxiliary leakage. In Pointcheval and Johansson [23], pages 117–134.

A Computing $g^{\mathbf{v}}$

We are given $\mathbf{F} \in \mathbb{Z}_q^{2\times 2\ell}$, $g^{\mathbf{D}} \in \mathbb{G}^{2\times 1}$ and want to compute $g^{\mathbf{v}} \in \mathbb{G}^{2\ell\times 1}$ where $\mathbf{Fv} = \mathbf{D}$. With all but negligible probability, we can assume that $\mathbf{F}$ as generated in our scheme is of rank 2. Solving the linear equation $\mathbf{Fv} = \mathbf{D}$ gives us

$$\left[\mathbf{I}_2 \middle| \mathbf{F}_1\right] \mathbf{v} = \mathbf{F}_2\mathbf{D}$$

where $\mathbf{I}_2$ is the 2×2 identity matrix, and $\mathbf{F}_1 \in \mathbb{Z}^{2\times(2\ell-2)}, \mathbf{F}_2 \in \mathbb{Z}_q^{2\times 2}$ depends on $\mathbf{F}$. Now let $\mathbf{w} = (\mathbf{v}[1], \mathbf{v}[2])^T$ and $\mathbf{w}' = (\mathbf{v}[3], \ldots, \mathbf{v}[2\ell])^T$ we have

$$\mathbf{w} + \mathbf{F}_1\mathbf{w}' = \mathbf{F}_2\mathbf{D},$$

so that $\mathbf{w}'$ can be free, and $\mathbf{w} = \mathbf{F}_2\mathbf{D} - \mathbf{F}_1\mathbf{w}'$. Since $g^{\mathbf{D}}$ is given, we can compute $g^{\mathbf{w}}$, and hence $g^{\mathbf{v}}$ as well.

B The probability λ in artificial abort

First define a binary function $\beta(id) = \begin{cases} 0 \text{ if } h_0 + \sum_{i=1}^{m} id[i]h_i = 0 \bmod J \\ 1 \text{ otherwise} \end{cases}$, and note that since q is exponential compared to mJ, we have

$$\alpha(id) = 0 \bmod q \Leftrightarrow h_0 + \sum_{i=1}^{m} id[i]h_i = kJ \bmod q \Leftrightarrow h_0 + \sum_{i=1}^{m} id[i]h_i = kJ$$
$$\Rightarrow h_0 + \sum_{i=1}^{m} id[i]h_i = 0 \bmod J \Leftrightarrow \beta(id) = 0$$

Since h_i are random in $\mathbb{Z}_J$, $\Pr[\beta(id) = 0] = 1/J$. Let $id_1, \ldots, id_Q$ are the extract queries, and note that the events $\beta(id_j) = 0$ and $\beta(id^*) = 0$ are pairwise independent for all $id_j \neq id^*$, we have

$$\begin{aligned}
\lambda &= \Pr\left[\left(\wedge_{j=1}^{Q}\alpha(id_j) \neq 0 \bmod q\right) \wedge \alpha(id^*) = 0 \bmod q\right] \\
&= \Pr\left[\left(\wedge_{j=1}^{Q}\beta(id_j) = 1\right) \wedge \sum_{i=1}^{m} id^*[i]h_i = kJ\right] = \frac{1}{m+1}\Pr\left[\left(\wedge_{j=1}^{Q}\beta(id_j) = 1\right) \wedge \beta(id^*) = 0\right] \\
&= \frac{1}{m+1}\Pr\left[\left(\wedge_{j=1}^{Q}\beta(id_j) = 1\right)\right]\Pr\left[\beta(id^*) = 0 \middle| \left(\wedge_{j=1}^{Q}\beta(id_j) = 1\right)\right] \\
&= \frac{1}{m+1}\left(1 - \Pr\left[\vee_{j=1}^{Q}\beta(id_j) = 0\right]\right)\Pr\left[\beta(id^*) = 0 \middle| \left(\wedge_{j=1}^{Q}\beta(id_j) = 1\right)\right] \\
&\geq \frac{1}{m+1}\left(1 - \sum_{j=1}^{Q}\Pr\left[\beta(id_j) = 0\right]\right)\Pr\left[\beta(id^*) = 0 \middle| \left(\wedge_{j=1}^{Q}\beta(id_j) = 1\right)\right] \\
&= \frac{1}{m+1}\left(1 - \frac{Q}{J}\right)\Pr\left[\beta(id^*) = 0 \middle| \left(\wedge_{j=1}^{Q}\beta(id_j) = 1\right)\right] \\
&= \frac{1}{m+1}\left(1 - \frac{Q}{J}\right)\frac{\Pr\left[\beta(id^*) = 0\right]}{\Pr\left[\wedge_{j=1}^{Q}\beta(id_j) = 1\right]}\Pr\left[\wedge_{j=1}^{Q}\beta(id_j) = 1 \middle| \beta(id^*) = 0\right] \\
&\geq \frac{1}{(m+1)}\left(1 - \frac{Q}{J}\right)\frac{1}{J}\Pr\left[\wedge_{j=1}^{Q}\beta(id_j) = 1 \middle| \beta(id^*) = 0\right] \\
&\geq \frac{1}{(m+1)}\left(1 - \frac{Q}{J}\right)\frac{1}{J}\left(1 - \sum_{j=1}^{Q}\Pr\left[\beta(id_j) = 0 \middle| \beta(id^*) = 0\right]\right) \\
&\geq \frac{1}{(m+1)J}\left(1 - \frac{Q}{J}\right)^2 \geq \frac{1}{(m+1)J}\left(1 - 2\frac{Q}{J}\right),
\end{aligned}$$

as stated.