Leakage Resilient IBE and IPE schemes*

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

[1] Ibaraki University, Japan, kurosawa@mx.ibaraki.ac.jp
[2] NICT, Japan, phong@nict.go.jp

Abstract. We construct identity-based encryption (IBE) and inner product encryption (IPE) schemes under the decision linear (DLIN) or symmetric external Diffie-Hellman (SXDH) assumptions. Their private user keys are leakage-resilient in several scenarios. In particular,

- In the bounded memory leakage model (Akavia et al., TCC '09), our basic schemes reach the maximum-possible leakage rate $1 - o(1)$.
- In the continual memory leakage model (Brakerski et al., Dodis et al., FOCS '10), variants of the above schemes enjoy leakage rate at least $\frac{1}{2} - o(1)$. Among the results, we improve upon the work of Brakerski et al. by presenting adaptively secure IBE schemes.

Keywords: Identity-based Encryption, Inner Product Encryption, leakage resilience.

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. We will work in the following models of leakage:

- the bounded memory leakage model [4], which allows arbitrary leakage on the private key for once. This is a basic model of leakage.
- the continual memory leakage model [13, 17], which allows leakage on the private key in many period of time. The holder of the key can update his/her key if suspecting any danger on it.

Recall that in identity-based encryption, first asked by Shamir [31], 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. [4] and Alwen et al. [7,8] 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. [15] presented a leakage resilient IBE with the leakage rate 1/3 under the DBDH assumption. Here, the leakage rate is defined as

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

Also recall that inner product encryption [21] 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 $id_{\text{IBE}} = id'_{\text{IBE}}$ for some identities id_{IBE} and id'_{IBE}, just check whether the inner product between vectors $id = (1, id_{\text{IBE}})$ and $u = (id'_{\text{IBE}}, -1)$ equals 0. IPE also serves as an important tool for designing encryption scheme supporting queries on encrypted data [12], and disjunctions, polynomial evaluation [21]. IPE is a class of functional encryption, which is a very active research field thanks to their potentially-wide applications.

* A preliminary version of this paper was presented at the 11th International Conference on Applied Cryptography and Network Security (ACNS '13) [23].

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. [15]	DBDH	$\|\mathsf{seed}\| + 3$	3	$1/3$
Lewko et al. [26]	$1, 2, 3$	L	L	$\frac{1}{1+c_1+c_3}(1 - O(1/L))$
Ours (Sect.4)	DLIN	2ℓ ($\ell \geq 3$)	2ℓ	$1 - \frac{3}{2\ell} - o(1)$
Ours (Sect.7)	SXDH	$2\ell'$ ($\ell' \geq 2$)	$2\ell'$	$1 - \frac{1}{\ell'} - o(1)$

Above, $c_1 = |p_1|/|p_2|, c_3 = |p_3|/|p_2|$ for some primes p_1, p_2, p_3, and $L \geq 4$. 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 [26] for details).

Table 2. IBE schemes in the CML model.

Schemes in CML model	Security	Memory leakage rate
Brakerski et al. [13]	selective	$\frac{1}{2} - o(1)$
Our DLIN-based IBE (Sect.6)	full	$\frac{1}{2} - o(1)$
Our SXDH-based IBE (Sect.7)	full	$1 - o(1)$

1.2 Our contributions

Our results and techniques are categorized and summarized as follows.

Contribution 1: IBE in bounded memory leakage model. We show leakage-resilient IBE schemes which achieve the maximum-possible leakage rate $1 - o(1)$ in the standard model under DLIN or SXDH assumptions. Precise values are in Table 1.

Technically, from the viewpoint of leakage resilience, our IBE scheme is based on the leakage resilient public key encryption scheme of Naor and Segev [28]. From the viewpoint of utilizing trapdoor in security reduction, it is 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 known to be leakage resilient. In fact, it seems hard to prove them leakage resilient; see Remark 1 below the proof of Theorem 3, but intuitively, the simulators of DLIN and SXDH have more freedom than that of [1].

Note also in Table 1, the IBE in Lewko et al. [26], while tolerating master key leakage, has private key leakage rate $\frac{1}{1+c}(1 - o(1))$ for $c = \frac{|p_1|+|p_3|}{|p_2|}$ (see the caption of Table 1). Simply taking $|p_1| \approx |p_2| \approx |p_3|$ yields a scheme with leakage rate $\frac{1}{3} - o(1)$. More sophisticated choices of c can help improving the rate, but decreasing the security level and/or causing difficulties in generating such pairing group.

Contribution 2: IPE in bounded memory leakage model. Going further, we propose the *first* leakage resilient IPE schemes in the literature. The schemes are selectively-secure, under the DLIN and SXDH assumptions respectively, with private key leakage rate $1 - o(1)$.

The design of our IPE scheme is partially inspired by the work of Agrawal et al. [3] in the lattice setting. Similarly to the above, the lattice-based counterpart is not known to be leakage resilient.

Contribution 3: extensions to the continual memory leakage model. Above are works in which the private keys are leaked, while arbitrarily, but once. Brakerski et al. [13] and Dodis et al. [17] considered the continual memory leakage (CML) model, and particularly the work [13] presented a selectively secure IBE scheme.

We show that our above schemes, with slight modifications, can be proved secure in the CML model. In particular, in the CML model, we present fully secure IBE schemes (see Table 2), and selectively secure IPE schemes.

1.3 Refinements over the conference version

An abridged version of this paper was in [23]. In this full version, we mainly refine the conference version in the following ways: (1) we add and analyze SXDH-based schemes, and (2) we conduct testing implementation on the basic DLIN-based schemes.

1.4 More related works

The CML-IBE scheme of Brakerski et al. [13] (under DLIN) can be seen as basing on Cash et al.'s IBE [14] (using lattices, not proven leakage resilient). The latter IBE is improved to obtain adaptive security in [1] in lattice setting (not proven leakage resilient). Our IBE schemes can be seen as [1]'s counterparts in DLIN setting.

Leakage models evolve in the literature. Some of them are motivated by practical issues, while others by theoretical needs. Choosing which model to use thus depends much on the environments running the schemes. We summarize some leakage models below.

- The "computation-leak-information" model was considered by Micali and Reyzin [27] to deal with physical observation via side channel attacks as in [22, 30]. One important axiom in this leakage model is that "*computation, and only computation, leaks information*". The reason given in [27] is: "*data can be placed in some form of storage where, when not being accessed and computed upon, it is totally secure.*"
- The bounded memory leakage model was examined in [4], to cope with the cold boot attack [20]. In this kind of attack, data in memory can be stolen while no computation is in process, and thus the above axiom of the "computation-leak-information" model is violated.
- The "floppy" model was introduced in [8] in which the leakage on secret keys can be continual if one relies on a leak-free source ("floppy" disk) updating the secret keys. Due to the use of a trusted external storage, this model is weaker than the CML model. In compensation, elegant schemes can be built without pairings as in [2].
- In the CML model, while there is no long-term, leak-free source, one need to assume that the randomness for updating secret keys is not totally leaked. In other words, these randomness can be seen as short-term, one-time "floppy". Initial works [13, 17] (and ours) tolerate logarithmic leakage amount on these randomness. Subsequent works [18, 24] improved on this topic by showing how to leak a constant fraction of the randomness for each local key update.
- The bottom-line of above models is that the secret key is still hard to recover given public parameters. The auxiliary-input model [16] considers exactly that. In other words, the leakage function can information-theoretically reveal the entire secret, provided that it is computationally infeasible to compute the secret. Yuen et al. [34] combined the CML model with the auxiliary-input model to create the continual auxiliary leakage (CAL) model.

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 [10], 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 [28, 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.

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.

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 $f(T)$.

We will also make use of the following lemma.

Lemma 2 (Leakage-resilient random subspaces [13]) *Let $m \geq l \geq 4$, and q be a prime. Let $\mathbf{X} \xleftarrow{\$} \mathbb{Z}_q^{m\times l}, \mathbf{T} \xleftarrow{\$} \mathbb{Z}_q^{l\times 2}, \mathbf{Y} \xleftarrow{\$} \mathbb{Z}_q^{m\times 2}$, and $f : \mathbb{Z}_q^{m\times 2} \to Z$. Then the statistical distance*

$$\Delta((\mathbf{X}, f(\mathbf{X} \cdot \mathbf{T})); (\mathbf{X}, f(\mathbf{Y}))) \leq \epsilon$$

as long as

$$|Z| \leq q^{l-3}\epsilon^2.$$

3 Definitions for IBE and IPE in the bounded leakage model

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 leakage rate.

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. Then the challenger runs Setup to generate (msk, pp), and sends pp to the adversary.*
2. **Private key generation***: the challenger runs $sk_{id^*} \leftarrow \mathsf{Extract}(msk, id^*)$.*
3. **Query set 1***: the adversary makes queries of the following types:*
   - *Extract queries $id \neq id^*$: the challenger returns $sk_{id} = \mathsf{Extract}(msk, id)$ to the adversary.*
   - *Leakage queries $(\mathtt{leak}, id, f)$ where id can be id^*, and f is some function: the challenger returns $f(sk_{id})$ to the adversary. These queries can be adaptive, and it is required that the sum (over all submitted functions f) of all lengths $|f(sk_{id})|$ 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}.*

4. **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 $b \xleftarrow{\$} \{0,1\}$.*
5. **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.*
6. **Finish:** *Finally, 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. *Initially, 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 $(\mathtt{leak}, id, f)$ where f is some function. The challenger returns $f(sk_{id})$ to the adversary. It is required that, for each identity id, the sum (over all submitted functions f) of all lengths $|f(sk_{id})|$ is less than $\rho_M |sk_{id}|$.*
   - *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***: the same as query set 1 above, except there is no extract or reveal query on id^*.*
5. **Challenge***: the adversary gives m_0, m_1 of equal length 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:** *Finally the adversary outputs a guess $b' \in \{0,1\}$. It succeeds if $b' = b$.*

Definition 3 (IBE in CML model, cf. [13]). *An IBE scheme is IND-ID-CPA secure in the CML model with leakage rate (ρ_U, 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:*
   - *Extraction queries $(\mathtt{extract}, id)$. The challenger returns $sk_{id,0} = \mathsf{Extract}(msk, id)$ to the adversary.*
   - *Leakage queries $(\mathtt{leak}, id, f)$ where f is a circuit. Initially, $L_{id,0} = 0$ and $i = 0$. If $L_{id,i} + |f(sk_{id,i})| \leq \rho_M \cdot |sk_{id,i}|$, the challenger returns $f(sk_{id,i})$ to the adversary and sets $L_i \leftarrow L_i + |f(sk_{id,i})|$. Otherwise the challenger aborts.*
   - *Update queries $(\mathtt{update}, f)$ for a circuit f. The challenger chooses randomness r for the updating process, and computes $f(sk_{id,i}, r)$. If either $|f(sk_{id,i}, r)| > \rho_U \cdot |sk_{id,i}|$ or $L_i + |f(sk_{id,i}, r)| > \rho_U \cdot |sk_{id,i}|$ then the challenge aborts. Otherwise it returns $f(sk_{id,i}, r)$ to the adversary and sets $sk_{id,i+1} \leftarrow \mathsf{Update}(sk_{id,i}, r)$, $L_{i+1} \leftarrow |f(sk_{id,i}, r)|$, and $i \leftarrow i + 1$.*
3. **Target identity:** *the adversary chooses target id^*, which did not appear in extract queries above.*
4. **Challenge:** *the adversary sends m_0, m_1 of the same length to the challenger, receiving the challenge ciphertext $c^* = \mathsf{Enc}(id^*, m_b)$ for a bit b chosen randomly by the challenger.*
5. **Query set 2:** *the adversary issues additional extraction queries $(\mathtt{extract}, id)$ with $id \neq id^*$ to which the challenger answers in the same manner as above.*
6. **Finish:** *the adversary outputs a guess $b' \in \{0,1\}$. It succeeds if $b' = b$.*

Inner product encryption. Consider algorithms (Setup, $\mathsf{Extract}$, Enc, 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. It is required that vectors id and u are of identical length. Decryption $\mathsf{Dec}(id, sk_{id}, c)$ works correctly if the inner product, defined over some group, between vectors id and u is 0, namely $\langle id, u\rangle = 0$. Define $\mathsf{Pred}_{id}(u) = \mathtt{true}$ (resp, $\mathtt{false}$) iff $\langle id, u\rangle = 0$ (resp, $\neq 0$).

Leakage resilient, selective security for IPE schemes are defined as follows.

Definition 4 (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. First, $\mathcal{A}$ announces attributes $u^{(0)}$, $u^{(1)}$. After that, $(mpk, msk) \leftarrow \mathsf{Setup}$, and mpk is given to $\mathcal{A}$.*

1. **Phase 1:** *$\mathcal{A}$ can ask extract query id to get sk_{id} as long as $\mathsf{Pred}_{id}(u^{(0)}) = \mathsf{Pred}_{id}(u^{(1)}) = \mathtt{false}$. $\mathcal{A}$ can also ask $(\mathtt{leak}, id, f)$ to obtain leakage $f(sk_{id})$. The condition is that the total length over all submitted f of all $|f(id)|$ 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 as long as $\mathsf{Pred}_{id}(u^{(0)}) = \mathsf{Pred}_{id}(u^{(1)}) = \mathtt{false}$.*
2. **Challenge:** *$\mathcal{A}$ submits equal-length $m^{(0)}, m^{(1)}$ for encryption. The challenger takes $b \xleftarrow{\$} \{0,1\}$, and sets $c^* = \mathsf{Enc}(u^{(b)}, m^{(b)})$.*
3. **Phase 2:** *$\mathcal{A}$ can ask for more extract queries as in Phase 1.*
4. **Finish:** *$\mathcal{A}$ return b' as a guess of b. Its advantage is defined as $|\Pr[b' = b] - 1/2|$.*

We above assume that $\mathsf{Pred}_{id}(u^{(0)}) = \mathsf{Pred}_{id}(u^{(1)}) = \mathtt{false}$ for all extract and leakage queries id. While the same restriction is also made in [3,25,29], it is stronger than the original definition in [21].

Definition 5 (Selectively secure IPE in CML model). *An IPE scheme is leakage resilient with leakage rate ρ_M, selectively secure in the CML model 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 $\mathsf{Pred}_{id}(u^{(0)}) = \mathsf{Pred}_{id}(u^{(1)}) = \mathtt{false}$. $\mathcal{A}$ can ask leakage queries $(\mathtt{leak}, id, f)$ where f is a circuit. Initially, $L_{id,0} = 0$ and $i = 0$. If $L_{id,i} + |f(sk_{id,i})| \leq \rho_M \cdot |sk_{id,i}|$, the challenger returns $f(sk_{id,i})$ to the adversary and sets $L_i \leftarrow L_i + |f(sk_{id,i})|$. Otherwise the challenger aborts.*
   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 as long as $\mathsf{Pred}_{id}(u^{(0)}) = \mathsf{Pred}_{id}(u^{(1)}) = \mathtt{false}$.
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.*
6. **Guess:** *$\mathcal{A}$ return b' as a guess of b. Its advantage is defined as $|\Pr[b' = b] - 1/2|$.*

4 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.

4.1 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 $C = g^{\mathbf{z}\cdot\mathbf{F}(id)},\ E = \hat{e}(g,g)^{\mathbf{z}\cdot\mathbf{D}}\cdot M$. Return (C, E) as the ciphertext.
– Dec: On input $sk_{id} = g^{\mathbf{v}}$ and $C = g^{\mathbf{c}}$, compute $K = \hat{e}(g,g)^{\mathbf{c}\cdot\mathbf{v}}$ 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: First randomly choose $\mathbf{w} \in \mathbb{Z}_q^{\ell\times 1}$. 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. 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 3 *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 (recalled in Section 3), 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,

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

so particularly $\mathbf{F}(id^*) = [\mathbf{A}_0|\mathbf{A}_0\mathbf{R}^*]$. $\mathcal{B}$ 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 $g^{\mathbf{A}_0}$. $\mathcal{B}$ then 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 $\mathsf{rank}(\mathbf{A}) = 3$. First 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 $\mathbf{Game}_0$. Now 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 $\mathbf{D} = \mathbf{F}(id^*) \cdot \mathbf{v}^*$, 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 $(\mathbf{c}^*, \mathbf{c}^*\mathbf{v}^*, f(\mathbf{v}^*))$ and $(\mathbf{c}^*, \mathsf{U}_{\mathbb{Z}_q}, f(\mathbf{v}^*))$ 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. □

4.2 On simulator comparison, and leakage rate computation

Below are some important notes.

Remark 1. In the above proof, the algorithm $\mathcal{B}$ against DLIN on input $g^{\mathbf{A}_0}$ 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 $\mathbf{v}^*$ is known to $\mathcal{B}$. In contrast, in the lattice based scheme of [1], the counterpart $\mathcal{B}$ against LWE has input $(\mathbf{A}_0, \mathbf{D})$, so it cannot choose $\mathbf{D}$, and hence cannot choose (short vector) $\mathbf{v}^*$ satisfying $\mathbf{D} = \mathbf{F}(id^*) \cdot \mathbf{v}^* (\mathrm{mod}\ q)$. Therefore, it seems hard to prove the lattice-based scheme leakage resilient.

Remark 2. 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., [11, Table 1]). This remark applies as well for estimating the leakage rate in the following sections.

4.3 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 4 *Employing the above $\mathbf{F}(id)$, the IBE scheme in Section 4.1 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 $1/2 - o(1)$.

Proof. At a high level, we utilize the artificial abort technique of Waters [33]. Note that one may also use the technique in [9] to improve the concrete security, in which artificial abort is not needed either.

Concretely, we construct simulator $\mathcal{B}$ against DLIN 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 [33, Sect.5.2, eq.(1k)], which is recapped in Section B for completeness. With 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 3 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 3.

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 $[\mathbf{I}_\ell \mid \mathbf{R}^*] \cdot \mathbf{v}^* = \mathbf{E}$ 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. □

5 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

$$msk = (\mathbf{A}_0, \ldots, \mathbf{A}_n)$$

and

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

– $\mathsf{Extract}_{msk}(id)$: Return $g^{\mathbf{v}} \in \mathbb{G}^{2\ell\times 1}$ where $\mathbf{F}(id)\cdot\mathbf{v} = \mathbf{D}$ for $\mathbf{F}(id) = [\mathbf{A}_0|\sum_{i=1}^n id_i\mathbf{A}_i]$.
– $\mathsf{Enc}(u, M \in \mathbb{G}_T)$: Take $\mathbf{z} \xleftarrow{\$} \mathbb{Z}_q^{1\times 2}$, return $C = g^{\mathbf{z}[\mathbf{A}_0|\mathbf{A}_1+u_1\mathbf{S}|\cdots|\mathbf{A}_n+u_n\mathbf{S}]}$ and $E = \hat{e}(g,g)^{\mathbf{z}\cdot\mathbf{D}}M$.
– $\mathsf{Dec}_{g^{\mathbf{v}}}(id, C, E)$: 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

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

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

Correctness. Following directly from below equations:

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

Theorem 5 *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: $\mathbf{Game}_0$ is the original attack game (described in Section 3); $\mathbf{Game}_1$ is the same, except that $\log_g C^* = [\mathbf{y}|\mathbf{y}_1|\cdots|\mathbf{y}_n]$ is chosen randomly. 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

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

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

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

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

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

Now suppose $\mathbf{A}$ 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 $\mathbf{y}, \mathbf{y}_1, \ldots, \mathbf{y}_n \xleftarrow{\$} \mathbb{Z}_q^{1\times\ell}$, $C^* = g^{[\mathbf{y}|\mathbf{y}_1|\cdots|\mathbf{y}_n]}$ and $E^* = \hat{e}(g,g)^{[\mathbf{y}|\sum_{i=1}^n id_i^*\mathbf{y}_i]\cdot\mathbf{v}^*} \cdot M^{(b)}$. 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 $\mathbb{Z}_q$. 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 $(\mathbf{c}^*, \mathbf{c}^*\mathbf{v}^*, f(\mathbf{v}^*))$ and $(\mathbf{c}^*, \mathsf{U}_{\mathbb{Z}_q}, f(\mathbf{v}^*))$, 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 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. □

6 Extensions to the CML model

Identity-based Encryption. To work in the CML model, we need to specify the algorithm $\mathsf{Update}_{\mathrm{user}}$ re-newing the private key of users. To do so, we choose $\mathbf{D} = \mathbf{0}$ working on $\ker(\mathbf{F}(id))$.

The private key for identity $id \in \{0,1\}^m$ is $g^{[\mathbf{v}_1|\mathbf{v}_2]}$ for $\mathbf{v}_i \xleftarrow{\$} \ker(\mathbf{F}(id))$. To renew the key, the user takes $\mathbf{S} \xleftarrow{\$} \mathbb{Z}_q^{2\times 2}$ and returns $g^{[\mathbf{v}_1|\mathbf{v}_2]\mathbf{S}}$. The nice effect of $\mathbf{D} = \mathbf{0}$ is that $[\mathbf{v}_1|\mathbf{v}_2]\mathbf{S}$ is also in the kernel space $\ker(\mathbf{F}(id)) \times \ker(\mathbf{F}(id))$ as required since

$$\mathbf{F}(id)[\mathbf{v}_1|\mathbf{v}_2]\mathbf{S} = [\mathbf{F}(id)\mathbf{v}_1|\mathbf{F}(id)\mathbf{v}_2]\mathbf{S} = \mathbf{0}.$$

However, due to $\mathbf{D} = \mathbf{0}$, we now have to consider an IBE scheme encrypting one bit. The scheme is described below, in which the parameter $\ell \geq 7$ (e.g., $\ell = 12$) affects the leakage rates.

- Setup: The public parameters are $pp = (g^{\mathbf{A}_0}, \ldots, g^{\mathbf{A}_m}, g^{\mathbf{B}})$ for $\mathbf{A}_0 \xleftarrow{\$} \mathbb{Z}_q^{2\times 3}$, and $\mathbf{A}_1, \ldots, \mathbf{A}_m$, $\mathbf{A}'_0 \xleftarrow{\$} \mathbb{Z}_q^{2\times(\ell-3)}$. The master secret key is set to $msk = (\mathbf{A}_0, \ldots, \mathbf{A}_m, \mathbf{A}'_0)$.
- Extract: For $id \in \{0,1\}^m$, $sk_{id} = g^{\mathbf{v}}$ where $\mathbf{v} = [\mathbf{v}_1|\mathbf{v}_2]$ in which $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{Z}_q^{\ell\times 1}$ satisfies

$$\mathbf{F}(id) \cdot \mathbf{v}_1 = \mathbf{F}(id) \cdot \mathbf{v}_2 = \mathbf{0}$$

  for

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

- $\mathsf{Update}_{\mathrm{user}}$: Choose $\mathbf{S} \xleftarrow{\$} \mathbb{Z}_q^{2\times 2}$ and return $sk'_{id} = g^{[\mathbf{v}_1|\mathbf{v}_2]\cdot\mathbf{S}}$.
- Enc: To encrypt $\mu \in \{0,1\}$, take $\mathbf{c} \xleftarrow{\$} \mathrm{span}(\mathbf{F}(id)) = \{\mathbf{z}\mathbf{F}(id) : \mathbf{z} \in \mathbb{Z}_q^{1\times 2}\}$ if $\mu = 0$; otherwise $\mathbf{c} \xleftarrow{\$} \mathbb{Z}_q^{1\times\ell}$. Return the ciphertext $g^{\mathbf{c}}$.
- Dec: To decrypt $g^{\mathbf{c}}$, compute $\hat{e}(g,g)^{\mathbf{c}\cdot\mathbf{v}}$. If the result is $\hat{e}(g,g)^{\mathbf{0}}$, then let $\mu = 0$, else $\mu = 1$.

Theorem 6 *The above IBE scheme is IND-ID-CPA-secure in the CML model under the DLIN assumption.*

Proof. Given an IND-ID-CPA adversary $\mathcal{A}$ against the scheme in the CML model, we build a simulator $\mathcal{B}$ against the DLIN assumption. The proof re-utilizes some ideas previously described. Specifically, $\mathcal{B}$ gets inputs $g^{\mathbf{A}}$ and $g^{\mathbf{y}}$ for $\mathbf{A} \in \mathbb{Z}_q^{2\times 3}, \mathbf{y} \in \mathbb{Z}_q^{1\times 3}$, and it will decide whether $\mathbf{y} \in \mathrm{span}(\mathbf{A})$. From $g^{\mathbf{A}}$, the simulator sets up $pp = (g^{\mathbf{A}_0}, \ldots, g^{\mathbf{A}_m}, g^{\mathbf{A}'_0})$ for the adversary $\mathcal{A}$ of the IBE scheme as follows.

$\mathcal{B}$ first sets $J = 4Q$, where Q is the number of extract queries of the adversary. $\mathcal{B}$ chooses $k \xleftarrow{\$} \{0, \ldots, m\}$ and $h_i \xleftarrow{\$} \mathbb{Z}_J$ for $i = 0, 1, \ldots, m$. It sets $\mathbf{A}_0 = \mathbf{A}\mathbf{Y}_1 \in \mathbb{Z}_q^{2\times 3}$ for $\mathbf{Y}_1 \xleftarrow{\$} \mathbb{Z}_q^{3\times 3}$. $\mathcal{B}$ 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 $\mathbf{C} \leftarrow \mathbb{Z}_q^{2\times(\ell-3)}$, and $\mathbf{R}_i \leftarrow \mathbb{Z}_q^{3\times(\ell-3)}$.

Note that as before

$$\begin{aligned}\mathbf{F}(id) &= \left[\mathbf{A}_0 \middle| \mathbf{A}'_0 + \sum_{i=1}^{m} id[i]\mathbf{A}_i\right] \\ &= \left[\mathbf{A}_0 \middle| \mathbf{A}_0(\mathbf{R}_0 + \sum_{i=1}^{m} id[i]\mathbf{R}_i) + \alpha(id)\mathbf{C}\right]\end{aligned}$$

for function

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

In case $\alpha(id) \neq 0$, $\mathcal{B}$ can answer extract queries id as follows. To find $g^{[\mathbf{v}_1|\mathbf{v}_2]}$ where $\mathbf{F}(id) \cdot \mathbf{v}_1 = \mathbf{F}(id) \cdot \mathbf{v}_2 = \mathbf{0}$, it lets

$$\mathbf{v}_1 = \begin{bmatrix} \mathbf{w}_1 - (\mathbf{R}_0 + \sum_{i=1}^{m} id[i]\mathbf{R}_i)\mathbf{x}_1 \\ \mathbf{x}_1 \end{bmatrix}, \mathbf{v}_2 = \begin{bmatrix} \mathbf{w}_2 - (\mathbf{R}_0 + \sum_{i=1}^{m} id[i]\mathbf{R}_i)\mathbf{x}_2 \\ \mathbf{x}_2 \end{bmatrix}$$

in which $\mathbf{w}_1, \mathbf{w}_2 \xleftarrow{\$} \mathbb{Z}_q^{3\times 1}$ and $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{Z}_q^{(\ell-3)\times 1}$ satisfies $\mathbf{A}_0\mathbf{w}_1 + \alpha(id)\mathbf{C}\mathbf{x}_1 = \mathbf{0}$ and $\mathbf{A}_0\mathbf{w}_2 + \alpha(id)\mathbf{C}\mathbf{x}_2 = \mathbf{0}$. The freedom of $\mathbf{x}_{1,2}$ is $(\ell-3)-2$, so that of corresponding $\mathbf{v}_{1,2}$ is $(\ell-3)-2+3 = \ell-2$, as expected. Leakage queries with circuit f are answered by returning $f(sk_{id}) = f(g^{[\mathbf{v}_1|\mathbf{v}_2]})$. Update queries with circuit f are answered by returning $f(sk_{id}, \mathbf{S}) = f(g^{[\mathbf{v}_1|\mathbf{v}_2]}, \mathbf{S})$ for $\mathbf{S} \xleftarrow{\$} \mathbb{Z}_q^{2\times 2}$.

In case $\alpha(id) = 0$, denote $id = id^*$ (the challenge identity). $\mathcal{B}$ sets

$$\mathbf{Y}_2 = \mathbf{Y}_1 \left(\mathbf{R}_0 + \sum_{i=1}^{m} id^*[i]\mathbf{R}_i \right).$$

Now take $\mathbf{X}' \xleftarrow{\$} \mathbb{Z}_q^{(\ell-3)\times(\ell-3)}$, and consider

$$\mathbf{X} = \begin{bmatrix} -(\mathbf{R}_0 + \sum_{i=1}^{m} id^*[i]\mathbf{R}_i) \cdot \mathbf{X}' \\ \mathbf{X}' \end{bmatrix} \in \mathbb{Z}_q^{\ell\times(\ell-3)},$$

we have for $\mathbf{Y} = [\mathbf{Y}_1|\mathbf{Y}_2] \in \mathbb{Z}_q^{3\times\ell}$,

$$\begin{aligned} \mathbf{Y}\mathbf{X} &= [\mathbf{Y}_1|\mathbf{Y}_2] \cdot \begin{bmatrix} -(\mathbf{R}_0 + \sum_{i=1}^{m} id^*[i]\mathbf{R}_i) \cdot \mathbf{X}' \\ \mathbf{X}' \end{bmatrix} \\ &= -\mathbf{Y}_1(\mathbf{R}_0 + \sum_{i=1}^{m} id^*[i]\mathbf{R}_i) \cdot \mathbf{X}' + \mathbf{Y}_2 \cdot \mathbf{X}' \\ &= \mathbf{0} \cdot \mathbf{X}' \\ &= \mathbf{0}. \end{aligned}$$

We claim that $\mathbf{X}$ is random. To prove, it suffices to show $\mathbf{R}_0\mathbf{X}' \in \mathbb{Z}_q^{3\times(\ell-3)}$ is random. This indeed holds true since $\mathbf{R}_0 \in \mathbb{Z}_q^{3\times(\ell-3)}$ is random and $\mathbf{X}'$ is invertible with all but negligible probability.

Also note that with high (namely, λ in Section B) probability,

$$\begin{aligned} \mathbf{F}(id^*) &= \left[\mathbf{A}_0 \middle| \mathbf{A}_0(\mathbf{R}_0 + \sum_{i=1}^{m} id^*[i]\mathbf{R}_i) \right] = \left[\mathbf{A}\mathbf{Y}_1 \middle| \mathbf{A}\mathbf{Y}_1(\mathbf{R}_0 + \sum_{i=1}^{m} id^*[i]\mathbf{R}_i) \right] \\ &= \left[\mathbf{A}\mathbf{Y}_1 \middle| \mathbf{A}\mathbf{Y}_2 \right] = \mathbf{A}\mathbf{Y} \end{aligned}$$

so that the challenge query will be answered by $g^{\mathbf{y}\mathbf{Y}}$.

Moreover, $\mathcal{B}$ can answer leakage and update queries on id^* using the target private key for period i as $sk_{id^*,i} = g^{\mathbf{X}\mathbf{S}_i}$, where $\mathbf{S}_i \xleftarrow{\$} \mathbb{Z}_q^{(\ell-3)\times 2}$. The leakage and update queries can be answered as in the following manner:

- Leakage query $(\texttt{leak}, f_i)$ for time period i: return $f_i(sk_{id^*,i})$.
- Update query $(\texttt{update}, f_i)$ for time period i: return $f_i(sk_{id^*,i}, \mathbf{S}_i)$ where $\mathbf{S}_i$ is as above.

Since all extract queries $id \neq id^*$ are answered correctly, the game now can be focuses on id^* as follows. The adversary attacks an PKE scheme described as follows:

- The public key is $pk = g^{\mathbf{F}(id^*)}$ and secret key $sk = g^{[\mathbf{v}_1|\mathbf{v}_2]}$ for $\mathbf{v}_i \xleftarrow{\$} \ker(\mathbf{F}(id^*))$.
- To update $sk = g^{[\mathbf{v}_1|\mathbf{v}_2]}$, take $\mathbf{S} \xleftarrow{\$} \mathbb{Z}_q^{2\times 2}$ and return $g^{[\mathbf{v}_1|\mathbf{v}_2]\mathbf{S}}$.

– The ciphertext for 0 is in the set $g^{\mathrm{span}(\mathbf{F}(id^*))}$, while that for 1 is chosen randomly from G^ℓ. To decrypt $g^{\mathbf{c}}$, compute $\hat{e}(g,g)^{\mathbf{c}[\mathbf{v}_1|\mathbf{v}_2]}$ using the bilinearity of the pairing.

This PKE is exactly the scheme $\mathcal{L}[\ell]$ in [13], recalled in Appendix C for completeness. The simulation thus goes on identically with the one in [13, full version, Sect.6.3]. Note also that the simulation in [13] requires that $\mathbf{X}$ is random in order to apply a type of leftover hash lemma (see [13, full version, Sect.2.1]), and yet this was already established above. Following the security of $\mathcal{L}[\ell]$ in the CML model (re-stated in Appendix C), the leakage rate tolerated by our scheme is

$$(\rho_U, \rho_M) = \left(\frac{c \log_2 |q|}{(2\ell+4)\log_2 q}, \frac{\ell - 6 - \gamma}{2\ell} \right)$$

for constants $c, \gamma > 0$. Taking $\ell = 12$ results in an IBE scheme secure in the CML model with memory leakage rate $\rho_M \approx 1/4$ (namely about 1/4 fraction of the private keys can be leaked), and the leakage amount tolerable for each update is $O(\log_2 |q|)$ (bits).

Inner Product Encryption. The scheme is described as follows. Setup takes $\mathbf{A}_{1\le i\le n}, \mathbf{S} \xleftarrow{\$} \mathbb{Z}_q^{2\times(\ell-3)}$, $\mathbf{A}_0 \xleftarrow{\$} \mathbb{Z}_q^{2\times 3}$, and lets $msk = (\mathbf{A}_0, \ldots, \mathbf{A}_n)$, $mpk = (g^{\mathbf{A}_0}, \ldots, g^{\mathbf{A}_n}, \mathbf{S})$. $\mathsf{Extract}_{msk}(id)$ for $id \in \mathbb{Z}_q^n \setminus \{(0,\ldots,0)\}$ returns $g^{\mathbf{v}} = g^{[\mathbf{v}_1|\mathbf{v}_2]} \in \mathbb{G}^{\ell\times 2}$ where with $j = 1, 2$,

$$\mathbf{F}(id) \cdot \mathbf{v}_j = \left[\mathbf{A}_0 \middle| \sum_{i=1}^n id_i \mathbf{A}_i \right] \cdot \mathbf{v}_j = \mathbf{0}.$$

$\mathsf{Update}_{\mathrm{user}}$ chooses $\mathbf{T} \xleftarrow{\$} \mathbb{Z}_q^{2\times 2}$ and returns $sk'_{id} = g^{[\mathbf{v}_1|\mathbf{v}_2]\cdot\mathbf{T}}$. Algorithm $\mathsf{Enc}(u, M \in \{0,1\})$ takes $\mathbf{z} \xleftarrow{\$} \mathbb{Z}_q^{1\times 2}$, and returns

$$C = g^{\mathbf{z}[\mathbf{A}_0|\mathbf{A}_1+u_1\mathbf{S}|\cdots|\mathbf{A}_n+u_n\mathbf{S}]}$$

if $M = 0$; otherwise choose $C \xleftarrow{\$} \mathbb{G}^{(\ell-3)n+3}$. $\mathsf{Dec}_{g^{\mathbf{v}}}(id, C = g^{[\mathbf{y}|\mathbf{y}_1|\cdots|\mathbf{y}_n]})$ computes $\prod_{i=1}^n (g^{\mathbf{y}_i})^{id_i} = g^{\sum_{i=1}^n id_i \mathbf{y}_i}$, 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 $F = \hat{e}(g,g)^{[\mathbf{y}|\sum_{i=1}^n id_i\mathbf{y}_i]\cdot\mathbf{v}} \in \mathbb{G}_T$ and output $M = 0$ if $F = \hat{e}(g,g)^{\mathbf{0}}$. Otherwise output $M = 1$.

Theorem 7 *The above IPE scheme is IND-sID-CPA-secure in the CML model under the DLIN assumption, with memory leakage rate* $1/2 - o(1)$.

Proof. We will consider the following games: $\mathbf{Game}_0$ is the original attack game (described in Section 3); $\mathbf{Game}_1$ is the same, except that $\log_g C^* = [\mathbf{y}|\mathbf{y}_1|\cdots|\mathbf{y}_n]$ is chosen randomly. 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 $g^{\mathbf{A}}, g^{\mathbf{y}}$ as inputs for $\mathbf{A} \in \mathbb{Z}_q^{2\times 3}$ and $\mathbf{y} \in \mathbb{Z}_q^{1\times 3}$, and will decide whether $\mathbf{y} = \mathbf{zA}$ or not. At first, $\mathcal{A}$ outputs $u^{(0)}, u^{(1)} \in \mathbb{Z}_q^n$. $\mathcal{B}$ considers $g^{\mathbf{A}_0} = g^{\mathbf{A}\mathbf{Y}_1}$ for random $\mathbf{Y}_1 \xleftarrow{\$} \mathbb{Z}_q^{3\times 3}$ chosen by $\mathcal{B}$. Then $\mathcal{B}$ sets for $1 \le i \le n$, $\mathbf{A}_i = \mathbf{A}_0\mathbf{R}_i^* - u_i^{(b)}\mathbf{S}$, where $b \xleftarrow{\$} \{0,1\}, \mathbf{R}_i^* \xleftarrow{\$} \mathbb{Z}_q^{3\times(\ell-3)}, \mathbf{S} \xleftarrow{\$} \mathbb{Z}_q^{2\times(\ell-3)}$ chosen by $\mathcal{B}$, and hence

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

Then $\mathcal{B}$ feeds $mpk = (g^{\mathbf{A}_0}, \ldots, g^{\mathbf{A}_n}, \mathbf{S})$ 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 $g^{\mathbf{v}} = g^{[\mathbf{v}_1|\mathbf{v}_2]}$ where $\mathbf{F}(id)\mathbf{v}_1 = \mathbf{F}(id)\mathbf{v}_2 = \mathbf{0}$. Since $\alpha \neq 0$, let $\mathbf{w}_1, \mathbf{w}_2 \xleftarrow{\$} \mathbb{Z}_q^{3\times 1}$, and set

$$\mathbf{v}_1 = \begin{bmatrix} \mathbf{w}_1 - (\sum_{i=1}^n id_i \mathbf{R}_i^*)\mathbf{x}_1 \\ \mathbf{x}_1 \end{bmatrix}, \mathbf{v}_2 = \begin{bmatrix} \mathbf{w}_2 - (\sum_{i=1}^n id_i \mathbf{R}_i^*)\mathbf{x}_2 \\ \mathbf{x}_2 \end{bmatrix}$$

where $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{Z}_q^{(\ell-3)\times 1}$ satisfies $\alpha\mathbf{S}\mathbf{x}_j = \mathbf{A}_0\mathbf{w}_j$ $(j = 0, 1)$ so that $g^{\mathbf{x}_j}$, and hence $g^{\mathbf{v}_j}$ can be computed by $\mathcal{B}$.

– **Leakage queries with** (id, f): if $\langle id, u^{(b)} \rangle \neq 0 \bmod q$, then similarly to the above simulation, $\mathcal{B}$ can generate sk_{id}, and then return $f(sk_{id})$ to $\mathcal{A}$. Therefore let us focus on the case $\langle id, u^{(b)} \rangle = 0 \bmod q$ in which now $\mathbf{F}(id) = [\mathbf{A}_0 | \mathbf{A}_0 \sum_{i=1}^{n} id_i \mathbf{R}_i^*] = \mathbf{A}\,[\mathbf{Y}_1 | \mathbf{Y}_1 \sum_{i=1}^{n} id_i \mathbf{R}_i^*]$. Now randomly take $\mathbf{X}' \xleftarrow{\$} \mathbb{Z}_q^{(\ell-3)\times(\ell-3)}$, and consider

$$\mathbf{X}_{id} = \begin{bmatrix} -(\sum_{i=1}^{m} id[i]\mathbf{R}_i^*) \cdot \mathbf{X}' \\ \mathbf{X}' \end{bmatrix} \in \mathbb{Z}_q^{\ell\times(\ell-3)},$$

so that $\mathbf{F}(id) \cdot \mathbf{X}_{id} = \mathbf{A} \cdot \mathbf{0} = \mathbf{0}$. The private key $sk_{id} = g^{\mathbf{v}_{id}}$ can be computed and returned to $\mathcal{A}$ by considering $\mathbf{v}_{id} = \mathbf{X}_{id}\mathbf{R}$ for random $\mathbf{R} \xleftarrow{\$} \mathbb{Z}_q^{(\ell-3)\times 2}$ chosen by $\mathcal{B}$.

– **Challenge query** $M^{(0)} = 0, M^{(1)} = 1$: $\mathcal{B}$ simply returns

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

If $\mathbf{y} = \mathbf{z}\mathbf{A}$ for some random $\mathbf{z} \in \mathbb{Z}_q^{1\times 2}$, we have

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

becoming an encryption of 0. Otherwise, if $\mathbf{y}$ is random independent of $\mathbf{A}$, C^* is random and hence becomes an encryption of 1.

– 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.

Revealing leakage on sk_{id} with $\langle id, u^{(b)} \rangle = 0 \mod q$ certainly raises a concern because these keys can decrypt the challenge ciphertext. We need to ensure these leakage information is harmless by restricting its amount. Applying Lemma 2 with subspace $\mathbf{X} = \mathbf{X}_{id} \in \mathbb{Z}_q^{\ell\times(\ell-3)}$, we need to set the leakage amount $|Z| \leq q^{(\ell-3)-3}2^{-2\eta}$ for statistical distance $2^{-\eta}$. This means the memory leakage rate tolerated is

$$\frac{(\ell-6)\log_2 q - 2\eta}{2\ell \log_2 q} = \frac{1}{2} - o(1)$$

as ℓ increases. □

7 Variant schemes based on SXDH

In this section, we work on *asymmetric* pairing groups $(G_1, G_2, G_T, g_1, g_2, \hat{e})$ where g_1, g_2 are generators of G_1, G_2, with pairing $\hat{e} : G_1 \times G_2 \to G_T$ and $G_1 \neq G_2$. The SXDH assumption intuitively say the decisional Diffie-Hellman assumption holds on both groups G_1 and G_2. In matrix language, it is hard to distinguish rank-1 and rank-2 matrices given in the exponent in both G_1 and G_2. More precisely, for all poly-time distinguishers $\mathcal{D}$, the advantage

$$\left| \Pr\left[b' = b : \begin{array}{l} \mathbf{U}_0 \xleftarrow{\$} \mathrm{Rk}_1(\mathbb{Z}_q^{2\times\ell}), \mathbf{U}_1 \xleftarrow{\$} \mathrm{Rk}_2(\mathbb{Z}_q^{2\times\ell}), \\ b \xleftarrow{\$} \{0,1\}, b' \leftarrow \mathcal{D}(g_1^{\mathbf{U}_b}, g_2^{\mathbf{U}_b}) \end{array} \right] - \frac{1}{2} \right|$$

is negligible under the SXDH assumption. Above, $\ell \geq 2$ can be any integer.

Selective IBE. The scheme is described as follows.

– Setup: Fix $\ell \geq 2$. The public parameters are $pp = (g_1^{\mathbf{A}_0}, g_1^{\mathbf{A}_1}, \mathbf{B}, g_1^d)$ for $\mathbf{A}_0, \mathbf{A}_1, \mathbf{B} \xleftarrow{\$} \mathbb{Z}_q^{1\times\ell}$ and $d \xleftarrow{\$} \mathbb{Z}_q$. The master secret key is $msk = (\mathbf{A}_0, \mathbf{A}_1)$.

– Extract: $sk_{id} = g_2^{\mathbf{v}}$ where $\mathbf{v} \in \mathbb{Z}_q^{2\ell\times 1}$ is a random vector such that $\mathbf{F}(id) \cdot \mathbf{v} = d$, for $\mathbf{F}(id) = [\mathbf{A}_0 | \mathbf{A}_1 + H(id)\mathbf{B}] \in \mathbb{Z}_q^{1\times 2\ell}$, where $H : \{0,1\}^* \to \mathbb{Z}_q$ is a collision-resistant hash function.

– Enc: To encrypt $M \in G_T$ under identity id, take $z \xleftarrow{\$} \mathbb{Z}_q$ and compute $C = g_1^{z\cdot\mathbf{F}(id)}, E = \hat{e}(g_1, g_2)^{zd}M$. Return (C, E) as the ciphertext.

– Dec: To decrypt (C, E) using $sk_{id} = g_2^{\mathbf{y}}$, compute $F = \hat{e}(C, sk_{id}) = \hat{e}(g_1, g_2)^{z\mathbf{F}(id)\mathbf{v}} = \hat{e}(g_1, g_2)^{zd}$. Return $M = F^{-1}E$.

Theorem 8 *The above IBE scheme is leakage-resilient IND-sID-CPA secure under the SXDH assumption with leakage rate* $1 - o(1)$.

Proof. The proof is quite similar to that of Theorem 3, so let us just outline the main ideas. The inputs to the simulator $\mathcal{B}$ are $(g_1^{\mathbf{x}}, g_1^{\mathbf{x}'}, g_2^{\mathbf{x}}, g_2^{\mathbf{x}'})$ for $\mathbf{x}, \mathbf{x}' \xleftarrow{\$} \mathbb{Z}_q^{1\times\ell}$, and it will decide whether $\mathbf{x}' = \alpha\mathbf{x}$ for some $\alpha \in \mathbb{Z}_q$. This corresponds to deciding whether matrix $\begin{bmatrix}\mathbf{x}\\ \mathbf{x}'\end{bmatrix} \in \mathbb{Z}_q^{2\times\ell}$ is of rank 1 or rank 2. After the adversary $\mathcal{A}$ announces id^*, $\mathcal{B}$ sets $g_1^{\mathbf{A}_0} = g_1^{\mathbf{x}}$ and considers $\mathbf{A}_1 = \mathbf{A}_0\mathbf{R}^* - H(id^*)\mathbf{B}$ for $\mathbf{R}^* \xleftarrow{\$} \mathbb{Z}_q^{\ell\times\ell}$ and $\mathbf{B} \xleftarrow{\$} \mathbb{Z}_q^{1\times\ell}$. $\mathcal{B}$ takes $\mathbf{v}^* \xleftarrow{\$} \mathbb{Z}_q^{2\ell\times 1}$ and sets $d = \mathbf{F}(id^*)\mathbf{v}^*$. $\mathcal{B}$ gives $pp = (g_1^{\mathbf{A}_0}, g_1^{\mathbf{A}_1}, \mathbf{B}, g_1^d)$ to $\mathcal{A}$. As before,

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

The answers to extract queries $id \neq id^*$ is $g_2^{\mathbf{y}}$ where $\mathbf{F}(id)\cdot\mathbf{v} = d$. Such $\mathbf{v}$ is constructed as

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

where $\mathbf{w} \xleftarrow{\$} \mathbb{Z}_q^{\ell\times 1}$ and random $\mathbf{w}' \in \mathbb{Z}_q^{\ell\times 1}$ satisfying $\mathbf{A}_0\mathbf{w} + (H(id) - H(id^*))\mathbf{B}\mathbf{w}' = d$. The knowledge of $g_2^{\mathbf{A}_0} = g_2^{\mathbf{x}}$ is used here to compute $g_2^{\mathbf{y}}$.

The challenge ciphertext consists of $C^* = g_1^{[\mathbf{x}'|\mathbf{x}'\mathbf{R}^*]}$, $E^* = \hat{e}(g_1, g_2)^{[\mathbf{x}'|\mathbf{x}'\mathbf{R}^*]\mathbf{v}^*} M_b$. If $\mathbf{x}' = \alpha\mathbf{x}$ then $[\mathbf{x}'|\mathbf{x}'\mathbf{R}^*] = \alpha[\mathbf{A}_0|\mathbf{A}_0\mathbf{R}^*]$, so that the ciphertext is legitimate. Otherwise $\mathbf{x}' \neq \alpha\mathbf{x}$, then $\begin{bmatrix}\mathbf{x}\\ \mathbf{x}'\end{bmatrix}$ is full-rank, we have $\mathbf{x}'\mathbf{R}^*$ is random and so does C^*. The rest of the proof goes a long those of Theorem 3. Since $\gamma(v^*) = q^{1-2\ell}$ the leakage rate is

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

approaching 1 as ℓ increases. □

We now describe other SXDH variants in the rest of this section, with their properties but without proofs, to avoid presenting essentially the same proofs twice.

Full IBE. By changing the function $\mathbf{F}(id)$ as in Sect.4.3, the above selective IBE can be turned into a fully secure one. More precisely, for $id \in \{0,1\}^m$,

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

where $\mathbf{A}_0, \mathbf{A}_1, \ldots, \mathbf{A}_m, \mathbf{A}_0' \in \mathbb{Z}_q^{1\times\ell}$ are random matrices employed as the master secret key. In the public parameters, the matrices are given in the exponents.

Inner Product Encryption. 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 $\mathbf{A}_i, \mathbf{S} \xleftarrow{\$} \mathbb{Z}_q^{1\times\ell}$ and $d \xleftarrow{\$} \mathbb{Z}_q$, let $msk = (\mathbf{A}_0, \ldots, \mathbf{A}_n)$, and $mpk = (g_1^{\mathbf{A}_0}, \ldots, g_1^{\mathbf{A}_n}, g_1^d, \mathbf{S})$.
– $\mathsf{Extract}_{msk}(id)$: Return $g_2^{\mathbf{y}} \in \mathbb{G}^{2\ell\times 1}$ where $\mathbf{F}(id)\cdot\mathbf{v} = \mathbf{D}$ for $\mathbf{F}(id) = [\mathbf{A}_0|\sum_{i=1}^n id_i\mathbf{A}_i]$.
– $\mathsf{Enc}(u, M \in \mathbb{G}_T)$: Take $z \xleftarrow{\$} \mathbb{Z}_q$, return $C = g_1^{z[\mathbf{A}_0|\mathbf{A}_1+u_1\mathbf{S}|\cdots|\mathbf{A}_n+u_n\mathbf{S}]}$ and $E = \hat{e}(g_1, g_2)^{zd}M$.

– $\mathsf{Dec}_{g^{\mathbf{v}}}(id, C, E)$: From $C = g_1^{[\mathbf{y}|\mathbf{y}_1|\cdots|\mathbf{y}_n]}$, compute

$$\prod_{i=1}^{n}(g_1^{\mathbf{y}_i})^{id_i} = g_1^{\sum_{i=1}^{n} id_i\mathbf{y}_i},$$

and hence obtain $g_1^{[\mathbf{y}|\sum_{i=1}^{n} id_i\mathbf{y}_i]}$. Pair that vector with the private key $g^{\mathbf{v}}$, obtaining $F = \hat{e}(g_1, g_2)^{[\mathbf{y}|\sum_{i=1}^{n} id_i\mathbf{y}_i]\cdot\mathbf{v}} \in \mathbb{G}_T$ and finally compute the message $M = E \cdot F^{-1}$.

Theorem 9 *The above IPE scheme is selectively secure under the SXDH assumption with memory leakage rate* $1 - o(1)$.

Full IBE in CML model.

– Setup: Fix $\ell \geq 4$. The public parameters are $pp = (g_1^{\mathbf{A}_0}, \ldots, g_1^{\mathbf{A}_m}, g_1^{\mathbf{B}})$ for $\mathbf{A}_0 \xleftarrow{\$} \mathbb{Z}_q^{1\times 1}$, and $\mathbf{A}_1, \ldots, \mathbf{A}_m$, $\mathbf{B} \xleftarrow{\$} \mathbb{Z}_q^{1\times(\ell-1)}$. The master secret key is $msk = (\mathbf{A}_0, \ldots, \mathbf{A}_m, \mathbf{B})$.
– $\mathsf{Extract}$: For $id \in \{0,1\}^m$, $sk_{id} = g_2^{\mathbf{y}}$ where $\mathbf{v} \in \mathbb{Z}_q^{\ell\times 1}$ satisfies

$$\mathbf{F}(id) \cdot \mathbf{v} = 0$$

for

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

– $\mathsf{Update}_{\text{user}}$: Choose $s \xleftarrow{\$} \mathbb{Z}_q$ and return $sk'_{id} = g_2^{s\cdot\mathbf{v}}$.
– Enc: To encrypt $\mu \in \{0,1\}$, let $\mathbf{c}^T \leftarrow \mathrm{span}(\mathbf{F}(id)) = \{z \cdot \mathbf{F}(id) : z \in \mathbb{Z}_q\}$ if $\mu = 0$; otherwise $\mathbf{c}^T \xleftarrow{\$} \mathbb{Z}_q^{1\times 4}$. Return the ciphertext $g_1^{\mathbf{c}^T}$.
– Dec: To decrypt $g_1^{\mathbf{c}^T}$, compute $\hat{e}(g_1, g_2)^{\mathbf{c}^T\cdot\mathbf{v}}$. If $\hat{e}(g_1, g_2)^{\mathbf{c}^T\cdot\mathbf{v}} = \hat{e}(g_1, g_2)^0$, then let $\mu = 0$, else $\mu = 1$.

Theorem 10 *The above scheme is IND-ID-CPA-secure in the CML model under the SXDH assumption with memory leakage rate* $1 - o(1)$.

IPE in CML model. Fix $\ell \geq 4$. Setup takes $\mathbf{A}_{1\leq i\leq n}, \mathbf{S} \xleftarrow{\$} \mathbb{Z}_q^{1\times(\ell-3)}$, $\mathbf{A}_0 \xleftarrow{\$} \mathbb{Z}_q^{1\times 1}$, and lets $msk = (\mathbf{A}_0, \ldots, \mathbf{A}_n)$, $mpk = (g_1^{\mathbf{A}_0}, \ldots, g_1^{\mathbf{A}_n}, \mathbf{S})$. $\mathsf{Extract}_{msk}(id)$ for $id \in \mathbb{Z}_q^n \setminus \{(0, \ldots, 0)\}$ returns $g_2^{\mathbf{y}}$ with $\mathbf{v} \in \mathbb{Z}_q^{\ell\times 1}$ where

$$\mathbf{F}(id) \cdot \mathbf{v} = \left[\mathbf{A}_0 \middle| \sum_{i=1}^{n} id_i\mathbf{A}_i\right] \cdot \mathbf{v} = 0.$$

$\mathsf{Update}_{\text{user}}$ chooses $t \xleftarrow{\$} \mathbb{Z}_q$ and returns $sk'_{id} = g^{t\cdot\mathbf{v}}$. Algorithm $\mathsf{Enc}(u, M \in \{0,1\})$ takes $z \xleftarrow{\$} \mathbb{Z}_q$, and returns

$$C = g_1^{z[\mathbf{A}_0|\mathbf{A}_1+u_1\mathbf{S}|\cdots|\mathbf{A}_n+u_n\mathbf{S}]}$$

if $M = 0$; otherwise choose random C as the encryption of $M = 1$. $\mathsf{Dec}_{g_2^{\mathbf{v}}}(id, C = g_1^{[\mathbf{y}|\mathbf{y}_1|\cdots|\mathbf{y}_n]})$ computes $\prod_{i=1}^{n}(g_1^{\mathbf{y}_i})^{id_i} = g_1^{\sum_{i=1}^{n} id_i\mathbf{y}_i}$, and hence obtain $g_1^{[\mathbf{y}|\sum_{i=1}^{n} id_i\mathbf{y}_i]}$. Pair that with the private key $g_2^{\mathbf{y}}$, obtaining $F = \hat{e}(g_1, g_2)^{[\mathbf{y}|\sum_{i=1}^{n} id_i\mathbf{y}_i]\cdot\mathbf{v}} \in \mathbb{G}_T$ and output $M = 0$ if $F = \hat{e}(g, g)^0$. Otherwise output $M = 1$.

Theorem 11 *The above IPE scheme is selectively secure in the CML model under the SXDH assumption with memory leakage rate* $1 - o(1)$.

8 Implementation

To obtain a sense on how our schemes perform on current computers, we prototype an implementation of our DLIN-based IBE schemes using Python with the Charm library [6]. Table 3 reports average running times after 10 trials using a laptop of moderate hardware (2.0 GHz CPU, 8 GB RAM) running Ubuntu 12.04 and Python 2.7.3.

Table 3. Running time of our DLIN-based IBE schemes with $\ell = 3$.

Schemes	Setup	Extract	Encryption	Decryption
Selective IBE	72 ms	23 ms	80 ms	23 ms
Full IBE	3760 ms	24 ms	67 ms	25 ms

The Setup algorithm of our full IBE is much slower than the one in selective IBE due to the use of Waters-like $F(id)$. Other algorithms of both perform similarly. Also note that, while Extract contains 6 exponetiations and Dec contains 6 pairings, the timings are almost the same. This is due to the version 0.42 of Charm we use does not optimize the computation of exponentation via pre-processing [5]. We take the 'SS512' pairing group (super-singular curve of 512-bit base field) in implementation.

References

1. S. Agrawal, D. Boneh, and X. Boyen. Efficient lattice (H)IBE in the standard model. In Gilbert [19], pages 553–572.
2. S. Agrawal, Y. Dodis, V. Vaikuntanathan, and D. Wichs. On continual leakage of discrete log representations. Cryptology ePrint Archive, Report 2012/367, 2012. `http://eprint.iacr.org/`. Accepted to Asiacrypt 2013.
3. 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.
4. 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.
5. J. A. Akinyele. Personal communication, 2013.
6. J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin. Charm: a framework for rapidly prototyping cryptosystems. *J. Cryptographic Engineering*, 3(2):111–128, 2013.
7. J. Alwen, Y. Dodis, M. Naor, G. Segev, S. Walfish, and D. Wichs. Public-key encryption in the bounded-retrieval model. In Gilbert [19], pages 113–134.
8. 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.
9. 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.
10. 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.
11. D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. *J. Cryptology*, 17(4):297–319, 2004.
12. 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.
13. 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 Trevisan [32], pages 501–510. Full version available at `http://eprint.iacr.org/2010/278.pdf`.
14. D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert. Bonsai trees, or how to delegate a lattice basis. In Gilbert [19], pages 523–552.
15. 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.

16. Y. Dodis, S. Goldwasser, Y. T. Kalai, C. Peikert, and V. Vaikuntanathan. Public-key encryption schemes with auxiliary inputs. In D. Micciancio, editor, *TCC*, volume 5978 of *Lecture Notes in Computer Science*, pages 361–381. Springer, 2010.
17. Y. Dodis, K. Haralambiev, A. López-Alt, and D. Wichs. Cryptography against continuous memory attacks. In Trevisan [32], pages 511–520.
18. Y. Dodis, A. B. Lewko, B. Waters, and D. Wichs. Storing secrets on continually leaky devices. In R. Ostrovsky, editor, *FOCS*, pages 688–697. IEEE, 2011.
19. 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.
20. J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten. Lest we remember: Cold boot attacks on encryption keys. In P. C. van Oorschot, editor, *USENIX Security Symposium*, pages 45–60. USENIX Association, 2008.
21. 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.
22. P. C. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In M. J. Wiener, editor, *CRYPTO*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397. Springer, 1999.
23. K. Kurosawa and L. T. Phong. Leakage resilient ibe and ipe under the dlin assumption. In M. J. J. Jr., M. E. Locasto, P. Mohassel, and R. Safavi-Naini, editors, *ACNS*, volume 7954 of *Lecture Notes in Computer Science*, pages 487–501. Springer, 2013.
24. A. B. Lewko, M. Lewko, and B. Waters. How to leak on key updates. In L. Fortnow and S. P. Vadhan, editors, *STOC*, pages 725–734. ACM, 2011.
25. 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 [19], pages 62–91.
26. A. B. Lewko, Y. Rouselakis, and B. Waters. Achieving leakage resilience through dual system encryption. In *TCC*, pages 70–88, 2011.
27. S. Micali and L. Reyzin. Physically observable cryptography (extended abstract). In M. Naor, editor, *TCC*, volume 2951 of *Lecture Notes in Computer Science*, pages 278–296. Springer, 2004.
28. 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`.
29. 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.
30. J.-J. Quisquater and D. Samyde. Electromagnetic analysis (EMA): Measures and counter-measures for smart cards. In I. Attali and T. P. Jensen, editors, *E-smart*, volume 2140 of *Lecture Notes in Computer Science*, pages 200–210. Springer, 2001.
31. A. Shamir. Identity-based cryptosystems and signature schemes. In *CRYPTO*, pages 47–53, 1984.
32. L. Trevisan, editor. *51th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2010, October 23-26, 2010, Las Vegas, Nevada, USA*. IEEE Computer Society, 2010.
33. 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.
34. T. H. Yuen, S. S. M. Chow, Y. Zhang, and S. M. Yiu. Identity-based encryption resilient to continual auxiliary leakage. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT*, volume 7237 of *Lecture Notes in Computer Science*, pages 117–134. Springer, 2012.

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.

C Public key encryption scheme $\mathcal{L}[\ell]$ in [13]

Description. Fix integer parameter $\ell \geq 7$. In key-generation, take random matrices $\mathbf{A} \in \mathbb{Z}_q^{2\times\ell}$ and $\mathbf{Y} \in \mathbb{Z}_q^{\ell\times 2}$ such that $\mathbf{AY} = \mathbf{0}$. The public key is $pk = g^{\mathbf{A}}$ and the secret key is $sk = g^{\mathbf{Y}}$. To update the secret key, take random $\mathbf{R} \in \mathbb{Z}_q^{2\times 2}$ and set $sk' = g^{\mathbf{YR}}$. Message space is of one bit. Encryption of bit 1 is $g^{\mathbf{u}}$ for random vector $\mathbf{u} \in \mathbb{Z}_q^{\ell}$. Encryption of bit 0 is $g^{\mathbf{rA}}$ for random vector $\mathbf{r} \in \mathbb{Z}_q^{1\times 2}$. In decryption, given a ciphertext $g^{\mathbf{c}}$ and secret key $g^{\mathbf{Y}}$, apply pairing $\hat{e}$ to get $\hat{e}(g,g)^{\mathbf{cY}}$. If the result equals $\hat{e}(g,g)^{\mathbf{0}}$, return 0, otherwise return 1 as the message.

Security in CML model [13, Theorem 6.1]. Under the DLIN assumption, for $\ell \geq 7$ and for all constants $\gamma, c > 0$, the above public key encryption scheme is secure in the CML model with update and memory leakage rates

$$(\rho_U, \rho_M) = \left(\frac{c \log_2 |q|}{(2\ell + 4) \log_2 q}, \frac{\ell - 6 - \gamma}{2\ell} \right).$$