Leakage Resilient IBE and IPE under the DLIN Assumption

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. 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.

Mentioned results are in the bounded memory leakage model (Akavia et al., TCC '09). We show that they naturally extends to the continual memory leakage model (Brakerski et al., Dodis et al., FOCS '10). In this stronger model, the leakage rate becomes $1/2 - o(1)$.

Keywords: IBE, IPE, 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. We will work in the following models of leakage: (1) the bounded memory leakage model of Akavia-Goldwasser-Vaikuntanathan [3], which allows arbitrary leakage on the private key for once. This is a basic model of leakage; and (2) the continual memory leakage model [12, 15], 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 [26], 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.

M. Jacobson et al. (Eds.): ACNS 2013, LNCS 7954, pp. 487–501, 2013.

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. [14] 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 [18] 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 [11], and disjunctions, polynomial evaluation [18]. 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 [23] showed a general functional encryption scheme under DLIN. These schemes include IBE and IPE. Some other IBE schemes under DLIN are in [6, 8, 19]. All of these schemes are not in any leakage 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, 18, 20, 23, 24], 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. 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. When ℓ grows, the leakage rate increases, while ciphertexts and private keys get longer.

Note also in Table 1, the IBE in Lewko et al. [21], 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 IBE scheme is based on the leakage resilient public key encryption scheme of Naor and Segev [22].

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

IBE Schemes	Assumption	Ctxt. overhead (group elements)	Priv. key (group elements)	Memory leakg. rate
Chow et al. [14]	DBDH	$\|\mathsf{seed}\| + 3$	3	$1/3$
Lewko et al. [21]	$1, 2, 3$	L	L	$\frac{1}{1+c_1+c_3}(1 - O(1/L))$
Ours (Sect.4)	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 [21] for details).

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 2, but intuitively, the simulator in DLIN setting has more freedom than that in lattice.

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. Similarly to the above, the lattice-based scheme is not known to be leakage resilient.

Extensions to the Continual Memory Leakage Model. Above are works in which the private keys are leaked, while arbitrarily, but once. Brakerski et al. [12] and Dodis et al. [15] considered the continual memory leakage (CML) model , and particularly [12] presented a selectively secure IBE scheme. Yuen et al. [29] in turn examined the (even more stronger) continual auxiliary input model, and proposed an IBE scheme fully secure under three static assumptions in composite order pairing groups (as in [21]).

We show that our above schemes, with slight modifications, can be proved secure in the CML model of [12]. In particular, in the CML model, we present a fully secure IBE scheme, and a selectively secure IPE scheme. (Note that the IBE scheme in [12] is selectively secure, while ours is fully secure.) While selectively secure, our IPE scheme is apparently the first one in the CML model.

Recently, Yuen et al. [29] considered the continual auxiliary leakage model, where, roughly speaking, the adversary is given leakage $f(sk)$ where function f

Table 2. IBE schemes in the CML model

Schemes in CML model	Security	Memory leakage rate
Brakerski et al. [12]	selective	$\frac{1}{2} - o(1)$
Our IBE (Sect.6)	full	$\frac{1}{2} - o(1)$

is computationally uninvertible. (The schemes are in the composite-order pairing groups.) Hence their setting is different from ours.

Relation of DLIN and Lattice-Based Schemes. The CML-IBE scheme of Brakerski et al. [12] (under DLIN) can be seen as basing on Cash et al.'s IBE [13] (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.

Roadmap. Section 4 is for IBE, while Section 5 is for IPE. Section 6 is for IBE and IPE in the CML model. To illustrate the main ideas, we start with a simple IBE scheme, which is selectively-secure and leakage-resilient, in Sect.4.1.

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 [22, 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. 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 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 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 $1/2$. In* **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. In* **private key generation***, the challenger runs $sk_{id^*} \leftarrow \mathsf{Extract}(msk, id^*)$. In* **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 (leak_i, id) where id can be id^*, and leak_i is some 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}.*

In **challenge** *phase, 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 $b \xleftarrow{\$} \{0, 1\}$. In* **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. 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) The challenger runs* Setup *to generate (msk, pp), and sends pp to the adversary. (2) In* **query set 1**, *the adversary makes queries of the following types:*

- *Extract queries id. The challenger returns the private key $sk_{id} =$ 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}.*

In **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.* **Query set 2** *is the 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 $\rho_M |sk_{id}|$. In* **challenge** *phase, 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 $b \xleftarrow{\$} \{0,1\}$. In* **query set 3**, *the adversary can ask more of extract queries $id \neq id^*$. Finally the adversary outputs a guess $b' \in \{0,1\}$. It succeeds if $b' = b$.*

Inner Product Encryption. Consider algorithms (Setup, 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. 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 $\mathsf{Pred}_{id}(u) =$ `true` (resp, `false`) iff $\langle id, u \rangle = 0$ (resp, $\neq 0$).

4 Proposed IBE Schemes under DLIN

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 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 (recalled in Appendix 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. □

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

4.2 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 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* $1/2 - o(1)$*.*

In the security reduction, we use the artificial abort technique of Waters [28]. (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 [28, Sect.5.2, eq.(1k)]. 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 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 $[\mathbf{I}_\ell \mid \mathbf{R}^*] \cdot \mathbf{v}^* = \mathbf{E}$ 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 $E = e(g,g)^{\mathbf{z}\cdot\mathbf{D}} M$.
- $\mathsf{Dec}_{g^{\mathbf{v}}}(id, C, E)$: 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: $[\mathbf{y}|\sum_{i=1}^n id_i \mathbf{y}_i] = [\mathbf{z}\mathbf{A}_0 | \mathbf{z}\sum_{i=1}^n id_i \mathbf{A}_i + \langle id, u \rangle \mathbf{z}\mathbf{S}] = [\mathbf{z}\mathbf{A}_0 | \mathbf{z}\sum_{i=1}^n id_i \mathbf{A}_i] = \mathbf{z}\mathbf{F}(id)$.

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.*

The proof will be given in the full version due to the lack of space.

6 Extensions to Continual Leakage

Identity-Based Encryption. To work in the CML model, following [12], we need to specify the algorithm $\mathsf{Update}_{\text{user}}$ 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., $\ell = 12$ for concreteness) affects the leakage rates. Below, security proofs are postponed to the full version due to space limit.

The IBE scheme is as follows. In Setup, the public params 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 $msk = (\mathbf{A}_0, \ldots, \mathbf{A}_m, \mathbf{A}'_0)$. $\mathsf{Extract}$, for input $id \in \{0,1\}^m$, returns $sk_{id} = g^{\mathbf{v}}$ 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

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

$\mathsf{Update}_{\text{user}}$ chooses $\mathbf{S} \xleftarrow{\$} \mathbb{Z}_q^{2\times 2}$ and returns $sk'_{id} = g^{[\mathbf{v}_1|\mathbf{v}_2]\cdot\mathbf{S}}$. Enc, encrypting $\mu \in \{0,1\}$, takes $\mathbf{c} \xleftarrow{\$} \text{span}(\mathbf{F}(id)) = \{\mathbf{z}\mathbf{F}(id) : \mathbf{z} \in \mathbb{Z}_q^{1\times 2}\}$ if $\mu = 0$; otherwise $\mathbf{c} \xleftarrow{\$} \mathbb{Z}_q^{1\times\ell}$, and returns the ciphertext $g^{\mathbf{c}}$. Dec, decrypting $g^{\mathbf{c}}$, computes $\hat{e}(g,g)^{\mathbf{c}\cdot\mathbf{v}}$ and if the result is $\hat{e}(g,g)^{\mathbf{0}}$, then returns $\mu = 0$, else returns $\mu = 1$.

Theorem 5. *The above IBE scheme is IND-ID-CPA-secure in the CML model under the DLIN assumption, with memory leakage rate* $1/2 - o(1)$.

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

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

$\mathsf{Update}_{\text{user}}$ 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 $F = e(g,g)^{[\mathbf{y}|\sum_{i=1}^{n} id_i\mathbf{y}_i]\cdot\mathbf{v}} \in \mathbb{G}_T$ and output $M = 0$ if $F = e(g,g)^{\mathbf{0}}$. Otherwise output $M = 1$.

Theorem 6. *The above IPE scheme is IND-sID-CPA-secure in the CML model under the DLIN assumption, with memory leakage rate* $1/2 - o(1)$.

References

1. Agrawal, S., Boneh, D., Boyen, X.: Efficient lattice (H)IBE in the standard model. In: Gilbert [16], pp. 553–572
2. Agrawal, S., Freeman, D.M., Vaikuntanathan, V.: 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. Akavia, A., Goldwasser, S., Vaikuntanathan, V.: Simultaneous hardcore bits and cryptography against memory attacks. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 474–495. Springer, Heidelberg (2009)
4. Alwen, J., Dodis, Y., Naor, M., Segev, G., Walfish, S., Wichs, D.: Public-key encryption in the bounded-retrieval model. In: Gilbert [16] pp. 113–134
5. Alwen, J., Dodis, Y., Wichs, D.: Survey: Leakage resilience and the bounded retrieval model. In: Kurosawa, K. (ed.) ICITS 2009. LNCS, vol. 5973, pp. 1–18. Springer, Heidelberg (2010)
6. Bellare, M., Kiltz, E., Peikert, C., Waters, B.: Identity-based (lossy) trapdoor functions and applications. In: Pointcheval, Johansson [25], pp. 228–245
7. Bellare, M., Ristenpart, T.: Simulation without the artificial abort: Simplified proof and improved concrete security for Waters' IBE scheme. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 407–424. Springer, Heidelberg (2009)
8. Bellare, M., Waters, B., Yilek, S.: Identity-based encryption secure against selective opening attack. In: Ishai [17], pp. 235–252
9. Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg (2004)
10. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the Weil pairing. J. Cryptology 17(4), 297–319 (2004)
11. Boneh, D., Waters, B.: Conjunctive, subset, and range queries on encrypted data. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 535–554. Springer, Heidelberg (2007)
12. Brakerski, Z., Kalai, Y.T., Katz, J., Vaikuntanathan, V.: Overcoming the hole in the bucket: Public-key cryptography resilient to continual memory leakage. In: Trevisan [27], pp. 501–510, Full version available at `http://eprint.iacr.org/2010/278.pdf`
13. Cash, D., Hofheinz, D., Kiltz, E., Peikert, C.: Bonsai trees, or how to delegate a lattice basis. In: Gilbert [16], pp. 523–552
14. Chow, S.S.M., Dodis, Y., Rouselakis, Y., Waters, B.: Practical leakage-resilient identity-based encryption from simple assumptions. In: Al-Shaer, E., Keromytis, A.D., Shmatikov, V. (eds.) ACM Conference on Computer and Communications Security, pp. 152–161. ACM (2010)

15. Dodis, Y., Haralambiev, K., López-Alt, A., Wichs, D.: Cryptography against continuous memory attacks. In: Trevisan [27], pp. 511–520
16. Gilbert, H. (ed.): EUROCRYPT 2010. LNCS, vol. 6110. Springer, Heidelberg (2010)
17. Ishai, Y. (ed.): TCC 2011. LNCS, vol. 6597. Springer, Heidelberg (2011)
18. Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 146–162. Springer, Heidelberg (2008)
19. Lewko, A.B.: Tools for simulating features of composite order bilinear groups in the prime order setting. In: Pointcheval, Johansson [25], pp. 318–335
20. Lewko, A.B., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In: Gilbert [16], pp. 62–91
21. Lewko, A.B., Rouselakis, Y., Waters, B.: Achieving leakage resilience through dual system encryption. In: Ishai [17], pp. 70–88
22. Naor, M., Segev, G.: Public-key cryptosystems resilient to key leakage. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 18–35. Springer, Heidelberg (2009), Full version available at `http://research.microsoft.com/en-us/um/people/gilse/papers/KeyLeakage.pdf`
23. Okamoto, T., Takashima, K.: Fully secure functional encryption with general relations from the decisional linear assumption. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 191–208. Springer, Heidelberg (2010)
24. Okamoto, T., Takashima, K.: Adaptively attribute-hiding (hierarchical) inner product encryption. In: Pointcheval, Johansson [25], pp. 591–608
25. Pointcheval, D., Johansson, T. (eds.): EUROCRYPT 2012. LNCS, vol. 7237, pp. 2012–2031. Springer, Heidelberg (2012)
26. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)
27. Trevisan, L. (ed.): 51th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2010, Las Vegas, Nevada, USA, October 23-26, 2010. IEEE Computer Society (2010)
28. Waters, B.: Efficient identity-based encryption without random oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005)
29. Yuen, T.H., Chow, S.S.M., Zhang, Y., Yiu, S.M.: Identity-based encryption resilient to continual auxiliary leakage. In: Pointcheval, Johansson [25], pp. 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.