Improved Inner-product Encryption with Adaptive Security and Full Attribute-hiding

Jie Chen[1,⋆], Junqing Gong[2,⋆⋆], and Hoeteck Wee[3,⋆⋆⋆]

[1] East China Normal University
s080001@e.ntu.edu.sg

[2] ENS de Lyon, Laboratoire LIP (U. Lyon, CNRS, ENSL, INRIA, UCBL)
junqing.gong@ens-lyon.fr

[3] CNRS and ENS, PSL
wee@di.ens.fr

Abstract. In this work, we propose two IPE schemes achieving both adaptive security and full attribute-hiding in the prime-order bilinear group, which improve upon the unique existing result satisfying both features from Okamoto and Takashima [Eurocrypt '12] in terms of efficiency.

- Our first IPE scheme is based on the standard k-LIN assumption and has shorter master public key and shorter secret keys than Okamoto and Takashima's IPE under weaker DLIN = 2-LIN assumption.
- Our second IPE scheme is adapted from the first one; the security is based on the XDLIN assumption (as Okamoto and Takashima's IPE) but now it also enjoys shorter ciphertexts.

Technically, instead of starting from composite-order IPE and applying existing transformation, we start from an IPE scheme in a very restricted setting but already in the *prime-order* group, and then gradually upgrade it to our full-fledged IPE scheme. This method allows us to integrate Chen *et al.*'s framework [Eurocrypt '15] with recent new techniques [TCC '17, Eurocrypt '18] in an optimized way.

1 Introduction

Attribute-based encryption (ABE) is an advanced public-key encryption system supporting fine-grained access control [31, 20]. In an ABE system, an authority publishes a master public key mpk for encryption and issues secret keys to users for decryption; a ciphertext for message m is associated with an attribute x while a secret key is associated with a policy f, a boolean function over the set of all attributes; when $f(x) = 1$, the secret key can be used to recover message m. The basic security requirement for ABE is *message-hiding*: an adversary holding a secret key with $f(x) = 0$ cannot infer any information about m from the ciphertext; furthermore, this should be ensured when the adversary has more than one such secret key, which is called *collusion resistance*.

In some applications, an additional security notion *attribute-hiding* [10, 22] is desirable, which concerns the privacy of attribute x instead of message m. In the literature, there are two levels of attribute-hiding: (1) *weak* attribute-hiding is against an adversary who holds multiple secret keys with $f(x) = 0$; (2) *full* attribute-hiding is against an adversary holding any kind of secret keys including those with $f(x) = 1$. Nowadays we have seen many concrete ABE schemes [20, 30, 7, 26, 24, 33, 25, 9, 18, 19, 21]. Based on the seminal *dual system method* [32], we even reached generic frameworks for constructing and analyzing ABE [4, 35, 11, 2, 5, 3, 6, 12] in bilinear groups. Many of them, including both concrete ABE schemes and generic frameworks, have already achieved weak attribute-hiding [9, 18, 19, 21, 11, 12].

However it is much harder to obtain ABE with the *full* attribute-hiding feature. In fact, all known schemes only support so-called inner-product encryption (IPE), in which both ciphertexts and secret keys

⋆ School of Computer Science and Software Engineering. Supported by the National Natural Science Foundation of China (Nos. 61472142, 61632012, U1705264) and the Young Elite Scientists Sponsorship Program by CAST (2017QNRC001). Homepage: http://www.jchen.top

⋆⋆ Supported in part by the French ANR ALAMBIC Project (ANR-16-CE39-0006).

⋆⋆⋆ Supported in part by the European Union's Horizon 2020 Research and Innovation Programme under grant agreement 780108 (FENTEC).

are associated with vectors and the decryption procedure succeeds when the two vectors has zero inner-product. Furthermore, almost all of them are selectively or semi-adaptively secure which means the adversary has to choose the vectors associated with the challenge ciphertext (called challenge vector/attribute) before seeing mpk or before seeing any secret keys [10, 22, 29, 36]. Both of them are much weaker than the standard *adaptive security* (i.e., the one we have mentioned in the prior paragraph) where the choice can be made at any time. (Note that Wee achieved *simulation-based* security in [36].) What's worse, some schemes [10, 22] are built on the composite-order group, on which group operations are slower and more memory space is required to store group elements. The best result so far comes from Okamoto and Takashima [27]: the IPE scheme is adaptively secure and fully attribute-hiding based on external decisional linear assumption[4] (XDLIN) in efficient prime-order bilinear groups.

1.1 Our Results

In this work, we propose two IPE schemes in prime-order bilinear groups achieving both adaptive security and full attribute-hiding, which improve upon Okamoto and Takashima's IPE scheme [27] in terms of space efficiency:

- Our first construction is proven secure under standard k-Linear (k-LIN) assumption. When instantiating with $k = 2$ (i.e., DLIN assumption), it enjoys shorter master public key and secret keys under weaker assumption than Okamoto and Takashima's IPE, but we have slightly larger ciphertexts. With parameter $k = 1$ (i.e., SXDH assumption), we can also achieve shorter ciphertexts but at the cost of basing the security on a stronger assumption.
- Our second construction is proven secure under the XDLIN assumption, which is stronger than DLIN assumption. This gives another balance point between (space) efficiency and assumption. Now we can get better efficiency than Okamoto and Takashima's IPE in terms of master public key, ciphertext and secret keys without sacrificing anything — Okamoto and Takashima also worked with XDLIN.

A detailed comparison is provided in Table 1.

Table 1. Comparison among our two IPE schemes and Okamoto and Takashima's IPE [27]. All schemes are built on an asymmetric prime-order bilinear group $(p, G_1, G_2, G_T, e : G_1 \times G_2 \to G_T)$. In the table, $|G_1|, |G_2|, |G_T|$ denote the sizes of group elements in G_1, G_2, G_T, respectively.

scheme	$\lvert\mathsf{mpk}\rvert$	$\lvert\mathsf{ct}\rvert$	$\lvert\mathsf{sk}\rvert$	assumption
OT12 [27]	$(12n+16)\lvert G_1\rvert + \lvert G_T\rvert$	$(5n+1)\lvert G_1\rvert + \lvert G_T\rvert$	$11\lvert G_2\rvert$	XDLIN
Sec. 3.4	$((2k^2+k)n+3k^2+2k)\lvert G_1\rvert + k\lvert G_T\rvert$	$((2k+1)n+k+1)\lvert G_1\rvert + \lvert G_T\rvert$	$(3k+2)\lvert G_2\rvert$	k-LIN
	$(10n+16)\lvert G_1\rvert + 2\lvert G_T\rvert$	$(5n+3)\lvert G_1\rvert + \lvert G_T\rvert$	$8\lvert G_2\rvert$	DLIN
	$(3n+5)\lvert G_1\rvert + \lvert G_T\rvert$	$(3n+2)\lvert G_1\rvert + \lvert G_T\rvert$	$5\lvert G_2\rvert$	SXDH
Sec. 4.4	$(8n+14)\lvert G_1\rvert + 2\lvert G_T\rvert$	$(4n+3)\lvert G_1\rvert + \lvert G_T\rvert$	$7\lvert G_2\rvert$	XDLIN

1.2 Our Technique in Composite-Order Groups

As a warm-up, we present a scheme in asymmetric composite-order bilinear groups. Here, we will rely on composite-order groups whose order is the product of *four* primes; this is different from the settings of

[4] The construction is originally based on the decisional linear assumption in *symmetric* prime-order bilinear group. In this paper, we will work with asymmetric bilinear group where their proof will be translated into a proof based on the external decisional linear assumption. Note that XDLIN assumption is stronger than DLIN assumption.

adaptively secure ABE schemes and selectively secure full attribute-hiding inner product encryption where it suffices to use *two* primes.

The scheme. Assume an asymmetric composite-order bilinear group $\mathbb{G} = (N, G_N, H_N, G_T, e : G_N \times H_N \to G_T)$ where $N = p_1 p_2 p_3 p_4$. Let g_1, h_{14} be respective random generators of subgroups $G_{p_1}, H_{p_1 p_4}$. Pick $\alpha, u, w_1, \ldots, w_n \leftarrow \mathbb{Z}_N$. We describe an IPE scheme for n dimensional space over $\mathbb{Z}_N$ as follows.

$$\begin{aligned}
\mathsf{mpk} &: g_1, g_1^u, g_1^{w_1}, \ldots, g_1^{w_n}, e(g_1, h_{14})^{\alpha} \\
\mathsf{sk}_{\mathbf{y}} &: h_{14}^{\alpha + (y_1 w_1 + \cdots + y_n w_n) r}, h_{14}^{r} \\
\mathsf{ct}_{\mathbf{x}} &: g_1^{s}, g_1^{s(u \cdot x_1 + w_1)}, \ldots, g_1^{s(u \cdot x_n + w_n)}, \mathsf{H}(e(g_1, h_{14})^{\alpha s}) \cdot m
\end{aligned} \tag{1}$$

where $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}_N^n$ and $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{Z}_N^n$. The construction is adapted from Chen *et al.* IPE [11] (without attribute-hiding feature) by embedding it into groups with four subgroups. This allows us to carry out the proof strategy introduced by Okamoto and Takashima [27], which involves a non-trivial extension of the standard dual system method [32]. We only give a high-level sketch for the proof below but show the complete game sequence in Fig 1 for reference.

As is the case for adaptively secure ABE [32, 35], we will rely on the following private-key one-ciphertext one-key fully attribute-hiding inner product encryption scheme in the proof of security. Here, g_3, h_3 denote the respective generators for the subgroups of order p_3.

$$\begin{aligned}
\mathsf{sk}_{\mathbf{y}} &: h_3^{\alpha + y_1 w_1 + \cdots + y_n w_n} \\
\mathsf{ct}_{\mathbf{x}} &: g_3^{u \cdot x_1 + w_1}, \ldots, g_3^{u \cdot x_n + w_n}, g_3^{\alpha} \cdot m
\end{aligned} \tag{2}$$

Note that the scheme satisfies (simulation-based) information-theoretic security in the selective setting, which immediately yields (indistinguishability-based) adaptive security via complexity leveraging.

In the proof of security (outlined in Fig 1), we will first switch the ciphertext to having just a $p_2 p_3 p_4$-component via the subgroup decision assumption. At the beginning of the proof, all the secret keys will have a p_4-component, and at the end, all the secret keys will have a p_2-component; throughout, the secret keys will also always have a p_1-component but no p_3-components at the beginning or the end. To carry out the change in the secret keys from p_4-components to p_2-components, we will switch the keys one by one. For the switch, we will introduce a p_3-component into one secret key and then invoke security of the above private-key one-ciphertext one-key scheme in the p_3-subgroup. It is important here that throughout the hybrids, at most one secret key has a p_3-component.

1.3 Our Technique in Prime-Order Groups

Assume a prime-order bilinear group $\mathbb{G} = (p, G_1, G_2, G_T, e : G_1 \times G_2 \to G_T)$ and let $[\cdot]_1, [\cdot]_2, [\cdot]_T$ denote the entry-wise exponentiation on G_1, G_2, G_T, respectively. Naively, we simulate a composite-order group whose order is the product of four primes using vectors of dimension $4k$ "in the exponent" under k-LIN assumption. That is, we replace

$$g_1, h_{14} \mapsto [\mathbf{A}_1]_1, [\mathbf{B}_{14}]_2$$

where $\mathbf{A}_1 \leftarrow \mathbb{Z}_p^{4k \times k}, \mathbf{B}_{14} \leftarrow \mathbb{Z}_p^{4k \times 2k}$. However, the resulting IPE scheme is less efficient than Okamoto and Takashima's scheme [27]. Instead, we will show that it suffices to use

$$\mathbf{A}_1 \leftarrow \mathbb{Z}_p^{(k+1) \times k}, \ \mathbf{B}_{14} \leftarrow \mathbb{Z}_p^{(2k+1) \times k} \tag{3}$$

Game	ct				κth sk: $H_{p_1} \times ?$			Remark
	$g_1^{s(u\cdot ?+w_i)}$	$g_2^{s(u\cdot ?+w_i)}$	$g_3^{s(u\cdot ?+w_i)}$	$g_4^{s(u\cdot ?+w_i)}$	$\kappa < j$	$\kappa = j$	$\kappa > j$	
0	$x_{i,b}$	—			H_{p_4}			Real game
1	—	$x_{i,b}$			H_{p_4}			$p_1 \mapsto p_2p_3p_4$ in G
$2.j-1$	—	$x_{i,0}$	$x_{i,b}$	$x_{i,b}$	H_{p_2}	H_{p_4}	H_{p_4}	
$2.j-1.1$	—	$x_{i,0}$	$x_{i,b}$	$x_{i,b}$	H_{p_2}	H_{p_3}	H_{p_4}	$p_4 \mapsto p_3$ in H
$2.j-1.2$	—	$x_{i,0}$	$x_{i,0}$	$x_{i,b}$	H_{p_2}	H_{p_3}	H_{p_4}	private-key scheme in p_3
$2.j-1.3$	—	$x_{i,0}$	$x_{i,0}$	$x_{i,b}$	H_{p_2}	H_{p_2}	H_{p_4}	$p_3 \mapsto p_2$ in H
3	—	$x_{i,0}$	$x_{i,0}$	$x_{i,0}$	H_{p_2}			statistical in p_3, p_4

Fig. 1. Game sequence for composite-order IPE. In the table, $\mathbf{x}_0 = (x_{1,0}, \ldots, x_{n,0})$ and $\mathbf{x}_1 = (x_{1,1}, \ldots, x_{n,1})$ are the challenge vectors; $b \in \{0,1\}$ is the secret bit we hope to hide against the adversary. The gray background highlights the difference between adjacent games. The column "ct" shows the structure of the challenge ciphertext on four subgroups whose generators are g_1, g_2, g_3, g_4, while the next column gives the subgroup where every secret keys lie in. In the last column, the notation "$p_1 \mapsto p_2p_3p_4$ in G" is indicating the subgroup decision assumption stating that $G_{p_1} \approx_c G_{p_2p_3p_4}$.

Then, with the correspondence by Chen *et al.* [11, 16, 13]:

$$\begin{aligned}
\alpha &\mapsto \mathbf{k} \in \mathbb{Z}_p^{k+1} & u, w_i &\mapsto \mathbf{U}, \mathbf{W}_i \in \mathbb{Z}_p^{(k+1)\times(2k+1)} \quad \forall i \in [n] \\
s &\mapsto \mathbf{s} \in \mathbb{Z}_p^k, & r &\mapsto \mathbf{r} \in \mathbb{Z}_p^k \\
g_1^s &\mapsto [\mathbf{s}^\top \mathbf{A}_1^\top]_1, & h_{14}^r &\mapsto [\mathbf{B}_{14}\mathbf{r}]_2 \\
g_1^{sw} &\mapsto [\mathbf{s}^\top \mathbf{A}_1^\top \mathbf{W}]_1, & h_{14}^{wr} &\mapsto [\mathbf{W}\mathbf{B}_{14}\mathbf{r}]_2
\end{aligned} \tag{4}$$

we have the following prime-order IPE scheme:

$$\begin{aligned}
\mathsf{mpk} &: [\mathbf{A}^\top]_1, [\mathbf{A}^\top \mathbf{U}]_1, [\mathbf{A}^\top \mathbf{W}_1]_1, \ldots, [\mathbf{A}^\top \mathbf{W}_n]_1, [\mathbf{A}^\top \mathbf{k}]_T \\
\mathsf{sk}_{\mathbf{y}} &: [\mathbf{k} + (y_1 \cdot \mathbf{W}_1 + \cdots + y_n \cdot \mathbf{W}_n)\mathbf{B}_{14}\mathbf{r}]_2,\ [\mathbf{B}_{14}\mathbf{r}]_2 \\
\mathsf{ct}_{\mathbf{x}} &: [\mathbf{s}^\top \mathbf{A}_1^\top]_1, [\mathbf{s}^\top \mathbf{A}_1^\top (x_1 \cdot \mathbf{U} + \mathbf{W}_1)]_1, \ldots, [\mathbf{s}^\top \mathbf{A}_1^\top (x_n \cdot \mathbf{U} + \mathbf{W}_n)]_1, [\mathbf{c}^\top \mathbf{k}]_T \cdot m
\end{aligned} \tag{5}$$

Note that, with matrices $\mathbf{A}_1 \in \mathbb{Z}_p^{(k+1)\times k}$ and $\mathbf{B} \in \mathbb{Z}_p^{(2k+1)\times k}$, we only simulate two and three subgroups, respectively, rather than four subgroups; meanwhile some of them are simulated as low-dimension subspaces. Although it has become a common optimization technique to adjust dimensions of subspaces, it is not direct to justify that we can work with less subspaces. In fact, these optimizations are based on elaborate investigations of the proof strategy sketched in Section 1.2. In the rest of this section, we explain our method leading to the optimized parameter shown in (3).

Our Translation. We start from an IPE scheme in a very restricted setting and then gradually upgrade it to our full-fledged IPE scheme in the *prime-order* group. In particular, we follow the roadmap

$$\text{private-key one-key IPE} \xrightarrow[\text{[11, 13]}]{\text{Step 1}} \text{private-key IPE} \xrightarrow[\text{[11, 36]}]{\text{Step 2}} \text{public-key IPE}$$

The private key one-key IPE corresponds to scheme (2) over p_3-subgroup (cf. $\mathsf{Game}_{2.j-1.2}$ in Fig 1). In Step 1, we move from one-key to multi-key model using the technique from [13], which is related to the argument just after we change ciphertext in proof of scheme (1) (cf. $\mathsf{Game}_{2.0}$ to $\mathsf{Game}_{2.q}$ and Game_3 in Fig 1). In Step 2, we move from private-key to public-key setting with the compiler in [36], which is related to the change of ciphertext at the beginning of the proof (cf. Game_1 in Fig 1). By handling these proof techniques underlying the proof sketched in Section 1.2 (cf. Fig 1) one by one as above, we are able to integrate Chen *et al.*'s framework [11] with recent new techniques [36, 13] in an optimized way.

Private-key IPE in One-key Setting. We start from a *private-key* IPE where the ciphertext is created from msk rather than mpk. We also consider a weaker *one-key* model where the adversary can get only one secret key. Pick $\alpha, u, w_1, \ldots, w_n \leftarrow_{\mathrm{R}} \mathbb{Z}_p$ and let message $m \in \mathbb{Z}_p$. We give the following private-key IPE over $\mathbb{Z}_p$:

$$\begin{aligned} &\mathsf{msk} : \alpha, u, w_1, \ldots, w_n \\ &\mathsf{sk}_{\mathbf{y}} : \alpha + (y_1 \cdot w_1 + \cdots + y_n \cdot w_n) \\ &\mathsf{ct}_{\mathbf{x}} : x_1 \cdot u + w_1, \ldots, x_n \cdot u + w_n, \alpha \cdot m \end{aligned} \tag{6}$$

Analogous to scheme (2), the scheme satisfies (simulation-based) information-theoretic security in the selective setting (cf. [36]). By the implication from simulation-based security to indistinguishability-based security and standard complexity leveraging technique, we have the following statement: For adaptively chosen $\mathbf{x}_0 = (x_{1,0}, \ldots, x_{n,0}) \in \mathbb{Z}_p^n$, $\mathbf{x}_1 = (x_{1,1}, \ldots, x_{n,1}) \in \mathbb{Z}_p^n$ and $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{Z}_p^n$ satisfying either $\langle \mathbf{x}_0, \mathbf{y} \rangle \neq 0 \wedge \langle \mathbf{x}_1, \mathbf{y} \rangle \neq 0$ or $\langle \mathbf{x}_0, \mathbf{y} \rangle = \langle \mathbf{x}_1, \mathbf{y} \rangle = 0$ and for all $b \in \{0, 1\}$, we have

$$\begin{aligned} &\{\boxed{x_{1,b}} \cdot u + w_1, \ldots, \boxed{x_{n,b}} \cdot u + w_n,\ y_1 \cdot w_1 + \cdots + y_n \cdot w_n\} \\ \equiv &\{\boxed{x_{1,1-b}} \cdot u + w_1, \ldots, \boxed{x_{n,1-b}} \cdot u + w_n,\ y_1 \cdot w_1 + \cdots + y_n \cdot w_n\} \end{aligned} \tag{7}$$

Note that the statement here is different from that used in Fig 1 (where $x_{i,0}$ is in the place of $x_{i,1-b}$). Looking ahead, this choice is made to employ the "change of basis" technique when moving from one-key to multi-key model (see the next paragraph).

Private-key IPE in Multi-key Setting. To handle multiple keys revealed to the adversary, we employ Chen *et al.*'s prime-order generic framework[5] [11] based on the dual system method [32] to scheme (6). The framework works with prime-order finite cyclic group G on which the k-LIN assumption holds. Let $[\cdot]$ denote the entry-wise exponentiation on G. In order to avoid collusion of multiple secret keys, we will re-randomize each secret key [8, 34, 31] using fresh vector $\mathbf{d} \leftarrow \mathsf{span}(\mathbf{B}_1)$ where $\mathbf{B}_1 \leftarrow \mathbb{Z}_p^{(k+1)\times k}$, which supports standard dual system method [32] with a hidden subspace $\mathbf{B}_2 \leftarrow \mathbb{Z}_p^{k+1}$. For this purpose, we need to do the following "scalar to vector" substitutions:

$$u \in \mathbb{Z}_p \mapsto \mathbf{u} \in \mathbb{Z}_p^{1\times(k+1)} \quad \text{and} \quad w_i \in \mathbb{Z}_p \mapsto \mathbf{w}_i \in \mathbb{Z}_p^{1\times(k+1)} \quad \forall i \in [n].$$

Then the re-randomization is done by multiplying $\mathbf{u}$ and each $\mathbf{w}_i$ in secret keys by $\mathbf{d}$ and moving them from $\mathbb{Z}_p$ to G. This yields the following private-key IPE:

$$\begin{aligned} &\mathsf{msk} : \alpha, \mathbf{u}, \mathbf{w}_1, \ldots, \mathbf{w}_n \\ &\mathsf{sk}_{\mathbf{y}} : [\alpha + (y_1 \cdot \mathbf{w}_1 + \cdots + y_n \cdot \mathbf{w}_n)\mathbf{d}],\ [\mathbf{d}] \quad \text{where} \quad \mathbf{d} \leftarrow \mathsf{span}(\mathbf{B}_1) \\ &\mathsf{ct}_{\mathbf{x}} : x_1 \cdot \mathbf{u} + \mathbf{w}_1, \ldots, x_n \cdot \mathbf{u} + \mathbf{w}_n, [\alpha] \cdot m \end{aligned} \tag{8}$$

To carry out the non-trivial extension by Okamoto and Takashima [27] which involves three subgroups of H_N (cf. game sequence from $\mathsf{Game}_{2.0}$ to $\mathsf{Game}_{2.q}$), we increase the dimension of vectors $\mathbf{u}, \mathbf{w}_1, \ldots, \mathbf{w}_n$, $\mathbf{d}$ in

[5] Note that, with their framework, we can work out a *public key* IPE directly, but we focus on the technique handling multiple secret keys at the moment.

secret keys by k (i.e., from $k+1$ to $2k+1$) as in [13] such that the support of $\mathbf{d}$ can accommodate three subspaces defined by

$$(\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3) \leftarrow \mathbb{Z}_p^{(2k+1)\times k} \times \mathbb{Z}_p^{2k+1} \times \mathbb{Z}_p^{(2k+1)\times k}$$

where $\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3$ play the roles similar to p_4, p_2, p_3-subgroup respectively. Following the proof strategy in [13] and statement (7) for the one-key scheme (6), we can change secret keys and the challenge ciphertext revealed to the adversary into the following form:

$$\begin{aligned}
&\mathsf{sk}_{\mathbf{y}} : [\alpha + (y_1 \cdot \mathbf{w}_1 + \cdots + y_n \cdot \mathbf{w}_n)\mathbf{d}],\ [\mathbf{d}] \quad \text{where} \quad \mathbf{d} \leftarrow \mathsf{span}(\mathbf{B}_1, \boxed{\mathbf{B}_2})\\
&\mathsf{ct}^* : x_{1,b} \cdot \mathbf{u}^{(1)} + \boxed{x_{1,1-b} \cdot \mathbf{u}^{(2)}} + x_{1,b} \cdot \mathbf{u}^{(3)} + \mathbf{w}_1, \ldots, x_{n,b} \cdot \mathbf{u}^{(1)} + \boxed{x_{n,1-b} \cdot \mathbf{u}^{(2)}} + x_{n,b} \cdot \mathbf{u}^{(3)} + \mathbf{w}_n,\ [\alpha] \cdot m
\end{aligned}$$

where $\mathbf{u}^{(1)}$ (resp. $\mathbf{u}^{(2)}$, $\mathbf{u}^{(3)}$) is a random vector orthogonal to $\mathsf{span}(\mathbf{B}_2, \mathbf{B}_3)$ (resp. $\mathsf{span}(\mathbf{B}_1, \mathbf{B}_3)$, $\mathsf{span}(\mathbf{B}_1, \mathbf{B}_2)$). Finally, by the "change of basis" commonly appeared in the proof with dual pairing vector space [23, 27] (and a simple statistical argument), we claim that ct^* has the same distribution as

$$\boxed{x_{1,0} \cdot \mathbf{u}_0 + x_{1,1} \cdot \mathbf{u}_1} + \mathbf{w}_1, \ldots, \boxed{x_{n,0} \cdot \mathbf{u}_0 + x_{n,1} \cdot \mathbf{u}_1} + \mathbf{w}_n,\ [\alpha] \cdot m$$

where $\mathbf{u}_0, \mathbf{u}_1 \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$. This means that ct^* hides b and scheme (8) is fully attribute-hiding.

Note that the support of randomness $\mathbf{d}$ (after the change) is $\mathsf{span}(\mathbf{B}_1, \mathbf{B}_2)$ rather than $\mathsf{span}(\mathbf{B}_2)$, which simulates p_2-subgroup in the composite-order scheme (1). This is crucial to derive more efficient IPE scheme but slightly complicates the final argument above where "change of basis" technique has to be used to deal with $x_{i,b} \cdot \mathbf{u}^{(1)}$ interplaying with $\mathbf{B}_1$-component in $\mathsf{sk}_{\mathbf{y}}$.

(Public-key) IPE scheme. To upgrade our private-key IPE to public-key IPE, we will employ the "private-key to public-key" compiler in [36]. The compiler relies on bilinear groups $(p, G_1, G_2, G_T, e : G_1 \times G_2 \to G_T)$ in which the k-LIN assumption holds. In detail, we do the following "vector to matrix"/"scalar to vector" substitution for entries in msk and secret keys:

$$\mathbf{u}, \mathbf{w}_1, \ldots, \mathbf{w}_n \in \mathbb{Z}_p^{1\times(2k+1)} \mapsto \mathbf{U}, \mathbf{W}_1, \ldots, \mathbf{W}_n \in \mathbb{Z}_p^{(k+1)\times(2k+1)}$$

$$\alpha \in \mathbb{Z}_p \mapsto \mathbf{k} \in \mathbb{Z}_p^{k+1}$$

and publish them as parts of mpk in the form of

$$[\mathbf{A}^\top \mathbf{U}]_1, [\mathbf{A}^\top \mathbf{W}_1]_1, \ldots, [\mathbf{A}^\top \mathbf{W}_n]_1, [\mathbf{A}^\top \mathbf{k}]_T \quad \text{where} \quad \mathbf{A} \leftarrow \mathbb{Z}_p^{(k+1)\times k}.$$

In the ciphertext, we translate $\mathbf{u}, \mathbf{w}_1, \ldots, \mathbf{w}_n$ into $[\mathbf{c}^\top \mathbf{U}]_1, [\mathbf{c}^\top \mathbf{W}_1]_1, \ldots, [\mathbf{c}^\top \mathbf{W}_n]_1$ where $\mathbf{c} \leftarrow \mathsf{span}(\mathbf{A})$ and translate $[\alpha]_2$ into $[\mathbf{c}^\top \mathbf{k}]_T$. Finally, secret keys are now moved to group G_2. This results in the following IPE scheme:

$$\begin{aligned}
&\mathsf{mpk} : [\mathbf{A}]_1, [\mathbf{A}^\top \mathbf{U}]_1, [\mathbf{A}^\top \mathbf{W}_1]_1, \ldots, [\mathbf{A}^\top \mathbf{W}_n]_1, [\mathbf{A}^\top \mathbf{k}]_T\\
&\mathsf{sk}_{\mathbf{y}} : [\mathbf{k} + (y_1 \cdot \mathbf{W}_1 + \cdots + y_n \cdot \mathbf{W}_n)\mathbf{d}]_2,\ [\mathbf{d}]_2 \qquad \text{where} \quad \mathbf{d} \leftarrow \mathsf{span}(\mathbf{B}_1)\\
&\mathsf{ct}_{\mathbf{x}} : [\mathbf{c}^\top]_1, [x_1 \cdot \mathbf{c}^\top \mathbf{U} + \mathbf{c}^\top \mathbf{W}_1]_1, \ldots, [x_n \cdot \mathbf{c}^\top \mathbf{U} + \mathbf{c}^\top \mathbf{W}_n]_1, [\mathbf{c}^\top \mathbf{k}]_T \cdot m \qquad \text{where} \quad \mathbf{c} \leftarrow \mathsf{span}(\mathbf{A})
\end{aligned} \tag{9}$$

Note that the translation does not involve $(\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3)$ we just introduced.

To prove the security of the resulting public-key IPE scheme, we first show that we can change the support of $\mathbf{c}$ from $\mathsf{span}(\mathbf{A})$ to $\mathbb{Z}_p^{k+1}$ by the following statement implied by the k-LIN assumption:

$$(\,[\mathbf{A}]_1, [\mathbf{c} \leftarrow \mathsf{span}(\mathbf{A})]_1\,) \approx_c (\,[\mathbf{A}]_1, [\mathbf{c} \leftarrow \mathbb{Z}_p^{k+1}]_1\,).$$

Since $(\mathbf{A} \,|\, \mathbf{c})$ is full-rank with overwhelming probability, we can see that

$$\widetilde{\mathsf{msk}} = (\mathbf{A}^\top \mathbf{U}, \mathbf{A}^\top \mathbf{W}_1, \ldots, \mathbf{A}^\top \mathbf{W}_n, \mathbf{A}^\top \mathbf{k}) \quad \text{and} \quad \mathsf{msk}^* = (\mathbf{c}^\top \mathbf{U}, \mathbf{c}^\top \mathbf{W}_1, \ldots, \mathbf{c}^\top \mathbf{W}_n, \mathbf{c}^\top \mathbf{k})$$

are distributed independently. Then the security of scheme (9) can be reduced to that of private-key scheme (8) by observations: (i) $\widetilde{\mathsf{msk}}$ is necessary for generating mpk in scheme (9); (ii) we can view a ciphertext in scheme (9) as a ciphertext of our private-key IPE scheme under master secret key msk^*; (iii) a secret key in scheme (9) can be produced from a secret key of private-key IPE scheme (8) under master secret key msk^* with the help of $\widetilde{\mathsf{msk}}$.

How to Shorten the Ciphertext. The ciphertext size of our IPE scheme (9) mainly depends on the width of matrix $\mathbf{U}$ and $\mathbf{W}_i$, which is further determined by the dimensions of subspaces defined by $\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3$. Therefore, in order to reduce the ciphertext size, we employ the "dimension compress" technique used in [16]. The basic idea is to let $\mathbf{B}_1$ and $\mathbf{B}_3$ "share some dimensions" and finally decrease the width of $\mathbf{U}$ and $\mathbf{W}_i$, the cost is that we have to use the XDLIN assumption. Compared with our first scheme, a qualitative difference is that the private-key variant now works with bilinear maps. This is not needed when we work with the k-LIN assumption in the first scheme.

Organization. The paper is organized as follows. In section 2, we review some basic notions. The next two sections, Section 3 and Section 4, will be devoted to our two IPE schemes, respectively. In both sections, we will first develop a private-key scheme and then transform it to the public-key version as [36].

2 Preliminaries

Notation. Let $\mathbf{A}$ be a matrix over $\mathbb{Z}_p$. We use $\mathsf{span}(\mathbf{A})$ to denote the column span of $\mathbf{A}$, use $\mathsf{basis}(\mathbf{A})$ to denote a basis of $\mathsf{span}(\mathbf{A})$, and use $(\mathbf{A}_1|\mathbf{A}_2)$ to denote the concatenation of matrices $\mathbf{A}_1, \mathbf{A}_2$. By $\mathsf{span}(\mathbf{A}^\top)$, we are indicating the row span of $\mathbf{A}^\top$. We let $\mathbf{I}_n$ be the n-by-n identity matrix and $\mathbf{0}$ be a zero matrix of proper size. Given an invertible matrix $\mathbf{B}$, we use $\mathbf{B}^*$ to denote its dual satisfying $\mathbf{B}^\top\mathbf{B}^* = \mathbf{I}$.

2.1 Inner-product encryption

Algorithms. An inner-product encryption (IPE) scheme consists of four algorithms $(\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$:

$\mathsf{Setup}(1^\lambda, n) \to (\mathsf{mpk}, \mathsf{msk})$. The setup algorithm gets as input the security parameter λ and the dimension n of the vector space. It outputs the master public key mpk and the master key msk.

$\mathsf{KeyGen}(\mathsf{msk}, \mathbf{y}) \to \mathsf{sk}_{\mathbf{y}}$. The key generation algorithm gets as input msk and a vector $\mathbf{y}$. It outputs a secret key $\mathsf{sk}_{\mathbf{y}}$ for vector $\mathbf{y}$.

$\mathsf{Enc}(\mathsf{mpk}, \mathbf{x}, m) \to \mathsf{ct}_{\mathbf{x}}$. The encryption algorithm gets as input mpk, a vector $\mathbf{x}$ and a message m. It outputs a ciphertext $\mathsf{ct}_{\mathbf{x}}$ for vector $\mathbf{x}$.

$\mathsf{Dec}(\mathsf{ct}_{\mathbf{x}}, \mathsf{sk}_{\mathbf{y}}) \to m$. The decryption algorithm gets as a ciphertext $\mathsf{ct}_{\mathbf{x}}$ for $\mathbf{x}$ and a secret key $\mathsf{sk}_{\mathbf{y}}$ for vector $\mathbf{y}$ satisfying $\langle \mathbf{x}, \mathbf{y} \rangle = 0$. It outputs message m.

Correctness. We require that for all vectors $\mathbf{x}, \mathbf{y}$ satisfying $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ and all m, it holds that

$$\Pr[\mathsf{Dec}(\mathsf{ct}_{\mathbf{x}}, \mathsf{sk}_{\mathbf{y}}) = m] = 1,$$

where $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda, n)$, $\mathsf{ct}_{\mathbf{x}} \leftarrow \mathsf{Enc}(\mathsf{mpk}, \mathbf{x}, m)$ and $\mathsf{sk}_{\mathbf{y}} \leftarrow \mathsf{KeyGen}(\mathsf{msk}, \mathbf{y})$.

Security. For a stateful adversary $\mathcal{A}$, we define the advantage function

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{IPE}}(\lambda) := \left| \Pr\left[b = b' : \begin{array}{l} (\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda, n); \\ (\mathbf{x}_0, \mathbf{x}_1, m_0, m_1) \leftarrow \mathcal{A}^{\mathsf{KeyGen}(\mathsf{msk}, \cdot)}(\mathsf{mpk}); \\ b \leftarrow_{\mathrm{R}} \{0,1\};\ \mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{mpk}, \mathbf{x}_b, m_b); \\ b' \leftarrow \mathcal{A}^{\mathsf{KeyGen}(\mathsf{msk}, \cdot)}(\mathsf{ct}^*) \end{array} \right] - \frac{1}{2} \right|$$

with the following restrictions on all queries $\mathbf{y}$ that $\mathcal{A}$ submitted to $\mathsf{KeyGen}(\mathsf{msk}, \cdot)$:

- if $m_0 \neq m_1$, we require that $\langle \mathbf{x}_0, \mathbf{y} \rangle \neq 0 \wedge \langle \mathbf{x}_1, \mathbf{y} \rangle \neq 0$;
- if $m_0 = m_1$, we require that either $\langle \mathbf{x}_0, \mathbf{y} \rangle \neq 0 \wedge \langle \mathbf{x}_1, \mathbf{y} \rangle \neq 0$ or $\langle \mathbf{x}_0, \mathbf{y} \rangle = \langle \mathbf{x}_1, \mathbf{y} \rangle = 0$.

An IPE scheme is *adaptively secure* and *fully attribute-hiding* if for all PPT adversaries $\mathcal{A}$, the advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathrm{IPE}}(\lambda)$ is a negligible function in λ.

Private-key IPE. In a private-key IPE, the Setup algorithm does not output mpk; and the Enc algorithm takes msk instead of mpk as input. The adaptive security and full attribute-hiding can be defined analogously except that $\mathcal{A}$ only gets ct^* and has access to $\mathsf{KeyGen}(\mathsf{msk}, \cdot)$. The advantage function is denoted by $\mathsf{Adv}_{\mathcal{A}}^{\mathrm{IPE}^*}(\lambda)$. Accordingly, we may call the standard IPE *public-key IPE*.

2.2 Prime-order groups and matrix Diffie-Hellman assumptions

A group generator $\mathcal{G}$ takes as input security parameter λ and outputs group description $\mathbb{G} = (p, G_1, G_2, G_T, e)$, where p is a prime of $\Theta(\lambda)$ bits, G_1, G_2 and G_T are cyclic groups of order p, and $e : G_1 \times G_2 \to G_T$ is a non-degenerate bilinear map. We require that group operations in G_1, G_2 and G_T as well the bilinear map e are computable in deterministic polynomial time with respect to λ. Let $g_1 \in G_1$, $g_2 \in G_2$ and $g_T = e(g_1, g_2) \in G_T$ be the respective generators. We employ the *implicit representation* of group elements: for a matrix $\mathbf{M}$ over $\mathbb{Z}_p$, we define $[\mathbf{M}]_1 = g_1^{\mathbf{M}}, [\mathbf{M}]_2 = g_2^{\mathbf{M}}, [\mathbf{M}]_T = g_T^{\mathbf{M}}$, where exponentiations are carried out component-wise. Given $\mathbf{A}$ and $[\mathbf{B}]_2$, we let $\mathbf{A} \odot [\mathbf{B}]_2 = [\mathbf{AB}]_2$; for $[\mathbf{A}]_1$ and $[\mathbf{B}]_2$, we let $e([\mathbf{A}]_1, [\mathbf{B}]_2) = [\mathbf{AB}]_T$.

We reivew the matrix Diffie-Hellman (MDDH) assumption on G_1 [14]. The $\mathrm{MDDH}_{k,\ell}$ assumption on G_2 can be defined analogously and it is known that $k\text{-LIN} \Rightarrow \mathrm{MDDH}_{k,\ell}$ [14].

Assumption 1 ($\mathrm{MDDH}_{k,\ell}$ Assumption) *Let $\ell > k \geq 1$. We say that the $\mathrm{MDDH}_{k,\ell}$ assumption holds with respect to $\mathcal{G}$ if for all PPT adversaries $\mathcal{A}$, the following advantage function is negligible in λ.*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{MDDH}_{k,\ell}}(\lambda) := |\Pr[\mathcal{A}(\mathbb{G}, [\mathbf{M}]_1, [\mathbf{Ms}]_1) = 1] - \Pr[\mathcal{A}(\mathbb{G}, [\mathbf{M}]_1, [\mathbf{u}]_1) = 1]|$$

where $\mathbb{G} \leftarrow \mathcal{G}(1^\lambda)$, $\mathbf{M} \leftarrow \mathbb{Z}_p^{\ell \times k}$, $\mathbf{s} \leftarrow \mathbb{Z}_p^k$ and $\mathbf{u} \leftarrow \mathbb{Z}_p^\ell$.

We also use the external decisional linear (XDLIN) assumption on G_2 [1]:

Assumption 2 (XDLIN Assumption) *We say that the XDLIN assumption holds with respect to $\mathcal{G}$ if for all PPT adversaries $\mathcal{A}$, the following advantage function is negligible in λ.*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{XDLIN}}(\lambda) := |\Pr[\mathcal{A}(\mathbb{G}, D, T_0 = [a_3(s_1 + s_2)]_2) = 1] - \Pr[\mathcal{A}(\mathbb{G}, D, T_1 \leftarrow G_2) = 1]|$$

where $\mathbb{G} \leftarrow \mathcal{G}(1^\lambda)$ and $D = ([a_1, a_2, a_3, a_1 s_1, a_2 s_2]_1, [a_1, a_2, a_3, a_1 s_1, a_2 s_2]_2)$ with $a_1, a_2, a_3, s_1, s_2 \leftarrow \mathbb{Z}_p$.

3 Construction from k-LIN assumption

3.1 Preparation

Fix parameters $\ell_1, \ell_2, \ell_3 \geq 1$ and let $\ell := \ell_1 + \ell_2 + \ell_3$. We use basis

$$\mathbf{B}_1 \leftarrow \mathbb{Z}_p^{\ell \times \ell_1},\ \mathbf{B}_2 \leftarrow \mathbb{Z}_p^{\ell \times \ell_2},\ \mathbf{B}_3 \leftarrow \mathbb{Z}_p^{\ell \times \ell_3},$$

and its dual basis $(\mathbf{B}_1^{\parallel}, \mathbf{B}_2^{\parallel}, \mathbf{B}_3^{\parallel})$ such that $\mathbf{B}_i^{\top}\mathbf{B}_i^{\parallel} = \mathbf{I}$ (known as *non-degeneracy*) and $\mathbf{B}_i^{\top}\mathbf{B}_j = \mathbf{0}$ if $i \neq j$ (known as *orthogonality*), as depicted in Fig 2.

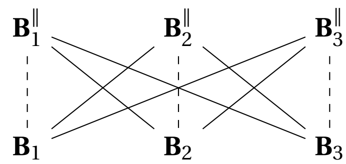

Fig. 2. Basis relations. Solid lines mean orthogonal, dashed lines mean non-degeneracy.

Assumption. We review the $\mathrm{SD}^{G_2}_{\mathbf{B}_1 \mapsto \mathbf{B}_1,\mathbf{B}_2}$ assumption [15, 17, 13] as follows. By symmetry, one may permute the indices for subspaces.

Lemma 1 **($\mathrm{MDDH}_{\ell_1,\ell_1+\ell_2} \Rightarrow \mathrm{SD}^{G_2}_{\mathbf{B}_1 \mapsto \mathbf{B}_1,\mathbf{B}_2}$).** *Under the* $\mathrm{MDDH}_{\ell_1,\ell_1+\ell_2}$ *assumption in* G_2*, there exists an efficient sampler outputting random* $([\mathbf{B}_1]_2, [\mathbf{B}_2]_2, [\mathbf{B}_3]_2)$ *(as described above) along with base* $\mathsf{basis}(\mathbf{B}_3^{\parallel})$ *and* $\mathsf{basis}(\mathbf{B}_1^{\parallel}, \mathbf{B}_2^{\parallel})$ *(of arbitrary choice) such that the following advantage function is negligible in* λ*.*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{SD}^{G_2}_{\mathbf{B}_1 \mapsto \mathbf{B}_1,\mathbf{B}_2}}(\lambda) := |\Pr[\mathcal{A}(\mathbb{G}, D, [\mathbf{t}_0]_1) = 1] - \Pr[\mathcal{A}(\mathbb{G}, D, [\mathbf{t}_1]_1) = 1]|$$

where

$$D := (\, [\mathbf{B}_1]_2, [\mathbf{B}_2]_2, [\mathbf{B}_3]_2, \mathsf{basis}(\mathbf{B}_1^{\parallel}, \mathbf{B}_2^{\parallel}), \mathsf{basis}(\mathbf{B}_3^{\parallel})\,)$$

$$\mathbf{t}_0 \leftarrow \mathsf{span}(\mathbf{B}_1),\ \mathbf{t}_1 \leftarrow \mathsf{span}(\mathbf{B}_1, \mathbf{B}_2).$$

Facts. With basis $(\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3)$, we can uniquely decompose $\mathbf{w} \in \mathbb{Z}_p^{1\times\ell}$ as

$$\mathbf{w} = \textstyle\sum_{\beta\in[3]} \mathbf{w}^{(\beta)} \quad \text{where} \quad \mathbf{w}^{(\beta)} \in \mathsf{span}(\mathbf{B}_\beta^{\parallel\,\top}).$$

In the paper, we use notation $\mathbf{w}^{(\beta)}$ to denote the projection of $\mathbf{w}$ onto $\mathsf{span}(\mathbf{B}_\beta^{\parallel\,\top})$ and define $\mathbf{w}^{(\beta_1\beta_2)} = \mathbf{w}^{(\beta_1)} + \mathbf{w}^{(\beta_2)}$ for $\beta_1, \beta_2 \in [3]$. Furthermore, we highlight two facts: (1) For $\beta \in [3]$, it holds that $\mathbf{w}\mathbf{B}_\beta = \mathbf{w}^{(\beta)}\mathbf{B}_\beta$; (2) For all $\beta^* \in [3]$, it holds that

$$\left\{ \boxed{\mathbf{w}^{(\beta^*)}}, \{\mathbf{w}^{(\beta)}\}_{\beta\neq\beta^*} \right\} \equiv \left\{ \boxed{\mathbf{w}^*}, \{\mathbf{w}^{(\beta)}\}_{\beta\neq\beta^*} \right\}$$

when $\mathbf{w} \leftarrow \mathbb{Z}_p^{1\times\ell}$ and $\mathbf{w}^* \leftarrow \mathsf{span}(\mathbf{B}_{\beta^*}^{\parallel\,\top})$.

3.2 Step One: A Private-key IPE in Prime-order Groups

Our first prime-order private-key IPE is described as follows. We use the basis described in Section 3.1 with $(\ell_1, \ell_2, \ell_3) = (k, 1, k)$. As mentioned in Section 1.2, we do not need bilinear map for this private-key IPE. However, for our future use in Section 3.4, we describe the IPE in bilinear groups and note that only one of source groups (i.e., G_2) is used.

– $\mathsf{Setup}(1^\lambda, n)$: Run $\mathbb{G} = (p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}(1^\lambda)$. Sample $\mathbf{B}_1 \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$ and pick $\mathbf{u}, \mathbf{w}_1, \ldots, \mathbf{w}_n \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$, $\alpha \leftarrow \mathbb{Z}_p$. Output

$$\mathsf{msk} = (\mathbb{G}, \alpha, \mathbf{u}, \mathbf{w}_1, \ldots, \mathbf{w}_n, \mathbf{B}_1).$$

– $\mathsf{KeyGen}(\mathsf{msk},\mathbf{y})$: Let $\mathbf{y}=(y_1,\ldots,y_n)\in\mathbb{Z}_p^n$. Sample $\mathbf{r}\leftarrow\mathbb{Z}_p^k$ and output

$$\mathsf{sk}_{\mathbf{y}}=(\,K_0=[\alpha+(y_1\cdot\mathbf{w}_1+\cdots+y_n\cdot\mathbf{w}_n)\mathbf{B}_1\mathbf{r}]_2,\,K_1=[\mathbf{B}_1\mathbf{r}]_2\,)$$

– $\mathsf{Enc}(\mathsf{msk},\mathbf{x},m)$: Let $\mathbf{x}=(x_1,\ldots,x_n)\in\mathbb{Z}_p^n$ and $m\in G_2$. Output

$$\mathsf{ct}_{\mathbf{x}}=(\,C_1=x_1\cdot\mathbf{u}+\mathbf{w}_1,\,\ldots,\,C_n=x_n\cdot\mathbf{u}+\mathbf{w}_n,\,C=[\alpha]_2\cdot m\,)$$

– $\mathsf{Dec}(\mathsf{ct}_{\mathbf{x}},\mathsf{sk}_{\mathbf{y}})$: Parse $\mathsf{ct}_{\mathbf{x}}=(C_1,\ldots,C_n,C)$ and $\mathsf{sk}_{\mathbf{y}}=(K_0,K_1)$ for $\mathbf{y}=(y_1,\ldots,y_n)\in\mathbb{Z}_p^n$. Output

$$m'=C\cdot((y_1\cdot C_1+\cdots+y_n\cdot C_n)\odot K_1)\cdot K_0^{-1}.$$

Correctness. For all $\mathbf{x},\mathbf{y}\in\mathbb{Z}_p^n$ satisfying $\langle\mathbf{x},\mathbf{y}\rangle=0$, we have

$$\begin{aligned}
&((y_1\cdot C_1+\cdots+y_n\cdot C_n)\odot K_1)\cdot K_0^{-1}\\
=\;&[(y_1\cdot(x_1\cdot\mathbf{u}+\mathbf{w}_1)+\cdots+y_n\cdot(x_n\cdot\mathbf{u}+\mathbf{w}_n))\mathbf{B}_1\mathbf{r}]_2\cdot[\alpha+(y_1\cdot\mathbf{w}_1+\cdots+y_n\cdot\mathbf{w}_n)\mathbf{B}_1\mathbf{r}]_2^{-1}\\
=\;&[\langle\mathbf{x},\mathbf{y}\rangle\cdot\mathbf{u}\mathbf{B}_1\mathbf{r}]_2\cdot[(y_1\cdot\mathbf{w}_1+\cdots+y_n\cdot\mathbf{w}_n)\mathbf{B}_1\mathbf{r}]_2\cdot[\alpha]_2^{-1}\cdot[(y_1\cdot\mathbf{w}_1+\cdots+y_n\cdot\mathbf{w}_n)\mathbf{B}_1\mathbf{r}]_2^{-1}=[\alpha]_2^{-1}
\end{aligned}$$

where the last equality follows from the fact that $\langle\mathbf{x},\mathbf{y}\rangle=0$. This readily proves the correctness.

3.3 Security of Private-key IPE

We will prove the following theorem.

Theorem 1. *Under the k-LIN assumption, the private-key IPE scheme described in Section 3.2 is adaptively secure and fully attribute-hiding (cf. Section 2.1).*

Following [35, 11], we can reduce the case $m_0\neq m_1$ to the case $m_0=m_1$ by arguing that an encryption for m_b is indistinguishable with an encryption for m_0. Therefore it is sufficient to prove the following lemma for $m_0=m_1$.

Lemma 2. *For any adversary $\mathcal{A}$ that makes at most Q key queries and outputs $m_0=m_1$, there exists adversaries $\mathcal{B}_1,\mathcal{B}_2,\mathcal{B}_3$ such that*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{IPE}^*}(\lambda)\le Q\cdot\mathsf{Adv}_{\mathcal{B}_1}^{\mathrm{SD}^{G_2}_{\mathbf{B}_1\mapsto\mathbf{B}_1,\mathbf{B}_3}}(\lambda)+Q\cdot\mathsf{Adv}_{\mathcal{B}_2}^{\mathrm{SD}^{G_2}_{\mathbf{B}_3\mapsto\mathbf{B}_3,\mathbf{B}_2}}(\lambda)+Q\cdot\mathsf{Adv}_{\mathcal{B}_3}^{\mathrm{SD}^{G_2}_{\mathbf{B}_1\mapsto\mathbf{B}_1,\mathbf{B}_3}}(\lambda)$$

and $\mathsf{Time}(\mathcal{B}_1),\mathsf{Time}(\mathcal{B}_2),\mathsf{Time}(\mathcal{B}_3)\approx\mathsf{Time}(\mathcal{A})$.

Game sequence. We prove Lemma 2 via the following game sequence, which is summarized in Fig 3.

– Game_0 is the real game in which the challenge ciphertext for $\mathbf{x}_b=(x_{1,b},\ldots,x_{n,b})$ is of the form

$$x_{1,b}\cdot\mathbf{u}+\mathbf{w}_1,\;\ldots,\;x_{n,b}\cdot\mathbf{u}+\mathbf{w}_n,\;[\alpha]_2\cdot m_0.$$

Here $b\leftarrow\{0,1\}$ is a secret bit.

– Game_1 is identical to Game_0 except that the challenge ciphertext is

$$x_{1,b}\cdot\mathbf{u}^{(13)}+\boxed{x_{1,1-b}\cdot\mathbf{u}^{(2)}}+\mathbf{w}_1,\;\ldots,\;x_{n,b}\cdot\mathbf{u}^{(13)}+\boxed{x_{n,1-b}\cdot\mathbf{u}^{(2)}}+\mathbf{w}_n,\;[\alpha]_2\cdot m_0.$$

We claim that $\mathsf{Game}_1\equiv\mathsf{Game}_0$. This follows from facts that (1) secret keys will not reveal $\mathbf{w}_1^{(2)},\ldots,\mathbf{w}_n^{(2)}$; (2) for all $\mathbf{x}_0,\mathbf{x}_1\in\mathbb{Z}_p^n$ and $\mathbf{u}^{(2)}\in\mathsf{span}(\mathbf{B}_2^{\|\top})$, it holds that

$$\{\boxed{x_{i,b}\cdot\mathbf{u}^{(2)}}+\mathbf{w}_i^{(2)}\}_{i\in[n]}\equiv\{\boxed{x_{i,1-b}\cdot\mathbf{u}^{(2)}}+\mathbf{w}_i^{(2)}\}_{i\in[n]}$$

when $\mathbf{w}_1^{(2)},\ldots,\mathbf{w}_n^{(2)}\leftarrow\mathsf{span}(\mathbf{B}_2^{\|\top})$. See Lemma 4 for more details.

Game	ct			κ-th sk ($\mathbf{d} \leftarrow$ span(?))			Remark
	$?^{(1)} + \mathbf{w}_i^{(1)}$	$?^{(2)} + \mathbf{w}_i^{(2)}$	$?^{(3)} + \mathbf{w}_i^{(3)}$	$\kappa < j$	$\kappa = j$	$\kappa > j$	
0	$x_{i,b} \cdot \mathbf{u}$			$\mathbf{B}_1$			Real game
1	$x_{i,b} \cdot \mathbf{u}$	$x_{i,1-b} \cdot \mathbf{u}$	$x_{i,b} \cdot \mathbf{u}$	$\mathbf{B}_1$			statistical argument: $\{x_{i,b} \cdot \mathbf{u}^{(2)} + \mathbf{w}_i^{(2)}\}_{i\in[n]} \equiv \{x_{i,1-b} \cdot \mathbf{u}^{(2)} + \mathbf{w}_i^{(2)}\}_{i\in[n]}$
$2.j-1$	$x_{i,b} \cdot \mathbf{u}$	$x_{i,1-b} \cdot \mathbf{u}$	$x_{i,b} \cdot \mathbf{u}$	$\mathbf{B}_1, \mathbf{B}_2$	$\mathbf{B}_1$	$\mathbf{B}_1$	$\mathsf{Game}_{2.0} = \mathsf{Game}_1$, $\mathsf{Game}_{2.j} = \mathsf{Game}_{2.j-1.5}$
$2.j-1.1$	$x_{i,b} \cdot \mathbf{u}$	$x_{i,1-b} \cdot \mathbf{u}$	$x_{i,b} \cdot \mathbf{u}$	$\mathbf{B}_1, \mathbf{B}_2$	$\mathbf{B}_1, \mathbf{B}_3$	$\mathbf{B}_1$	$\mathrm{SD}^{G_2}_{\mathbf{B}_1 \mapsto \mathbf{B}_1, \mathbf{B}_3}$: $[\mathsf{span}(\mathbf{B}_1)]_2 \approx_c [\mathsf{span}(\mathbf{B}_1, \mathbf{B}_3)]_2$ given $\mathsf{basis}(\mathbf{B}_2^{\parallel}), \mathsf{basis}(\mathbf{B}_1^{\parallel}, \mathbf{B}_3^{\parallel})$
$2.j-1.2$	$x_{i,b} \cdot \mathbf{u}$	$x_{i,1-b} \cdot \mathbf{u}$	$x_{i,1-b} \cdot \mathbf{u}$	$\mathbf{B}_1, \mathbf{B}_2$	$\mathbf{B}_1, \mathbf{B}_3$	$\mathbf{B}_1$	statistical argument: $\{x_{i,b} \cdot \mathbf{u}^{(3)} + \mathbf{w}_i^{(3)}\}_{i\in[n]} \equiv \{x_{i,1-b} \cdot \mathbf{u}^{(3)} + \mathbf{w}_i^{(3)}\}_{i\in[n]}$ given $y_1 \cdot \mathbf{w}_1^{(3)} + \cdots + y_n \cdot \mathbf{w}_n^{(3)}$
$2.j-1.3$	$x_{i,b} \cdot \mathbf{u}$	$x_{i,1-b} \cdot \mathbf{u}$	$x_{i,1-b} \cdot \mathbf{u}$	$\mathbf{B}_1, \mathbf{B}_2$	$\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3$	$\mathbf{B}_1$	$\mathrm{SD}^{G_2}_{\mathbf{B}_3 \mapsto \mathbf{B}_3, \mathbf{B}_2}$: $[\mathsf{span}(\mathbf{B}_3)]_2 \approx_c [\mathsf{span}(\mathbf{B}_2, \mathbf{B}_3)]_2$ given $\mathsf{basis}(\mathbf{B}_1^{\parallel}), \mathsf{basis}(\mathbf{B}_2^{\parallel}, \mathbf{B}_3^{\parallel})$
$2.j-1.4$	$x_{i,b} \cdot \mathbf{u}$	$x_{i,1-b} \cdot \mathbf{u}$	$x_{i,b} \cdot \mathbf{u}$	$\mathbf{B}_1, \mathbf{B}_2$	$\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3$	$\mathbf{B}_1$	statistical argument: analogous to $\mathsf{Game}_{2.j-1.2}$
$2.j-1.5$	$x_{i,b} \cdot \mathbf{u}$	$x_{i,1-b} \cdot \mathbf{u}$	$x_{i,b} \cdot \mathbf{u}$	$\mathbf{B}_1, \mathbf{B}_2$	$\mathbf{B}_1, \mathbf{B}_2$	$\mathbf{B}_1$	$\mathrm{SD}^{G_2}_{\mathbf{B}_1 \mapsto \mathbf{B}_1, \mathbf{B}_3}$: analogous to $\mathsf{Game}_{2.j-1.1}$
3	$x_{i,0} \cdot \mathbf{u}_0 + x_{i,1} \cdot \mathbf{u}_1$		$x_{i,b} \cdot \mathbf{u}$	$\mathbf{B}_1, \mathbf{B}_2$			$\mathbf{u}_0, \mathbf{u}_1 \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$; statistical argument: change of basis w.r.t. $\mathsf{span}(\mathbf{B}_1, \mathbf{B}_2)$
4	$x_{i,0} \cdot \mathbf{u}_0 + x_{i,1} \cdot \mathbf{u}_1$			$\mathbf{B}_1, \mathbf{B}_2$			statistical argument: analogous to $\mathsf{Game}_{2.j-1}$

Fig. 3. Game sequence for private-key IPE based on k-LIN assumption. The gray background highlights the difference between adjacent games. Here, $\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3$ play a role similar to the p_4, p_2, p_3-subgroups in Fig 1.

- $\mathsf{Game}_{2.j}$ for $j \in [0, q]$ is identical to Game_1 except that the first j secret keys are

$$[\alpha + (y_1 \cdot \mathbf{w}_1 + \cdots + y_n \cdot \mathbf{w}_n)\mathbf{d}]_2,\ [\mathbf{d}]_2 \quad \text{where} \quad \boxed{\mathbf{d} \leftarrow \mathsf{span}(\mathbf{B}_1, \mathbf{B}_2)}.$$

  We claim that $\mathsf{Game}_{2.j-1} \approx_c \mathsf{Game}_{2.j}$ for $j \in [q]$ and give a proof sketch later.
- Game_3 is identical to $\mathsf{Game}_{2.q}$ except that the challenge ciphertext is

$$\boxed{x_{1,0} \cdot \mathbf{u}_0^{(12)} + x_{1,1} \cdot \mathbf{u}_1^{(12)}} + x_{1,b} \cdot \mathbf{u}^{(3)} + \mathbf{w}_1,\ \ldots,\ \boxed{x_{n,0} \cdot \mathbf{u}_0^{(12)} + x_{n,1} \cdot \mathbf{u}_1^{(12)}} + x_{n,b} \cdot \mathbf{u}^{(3)} + \mathbf{w}_n,\ [\alpha]_2 \cdot m_0.$$

  where $\mathbf{u}_0, \mathbf{u}_1 \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$. We claim that $\mathsf{Game}_{2.q} \equiv \mathsf{Game}_3$. This follows from the "change of basis" technique used in dual pairing vector spaces [23, 28]. In particular, we argue that

$$(\overbrace{\mathbf{u}^{(1)}}^{x_{i,b}}, \overbrace{\mathbf{u}^{(2)}}^{x_{i,1-b}}) \equiv (\mathbf{u}_0^{(12)}, \mathbf{u}_1^{(12)})$$

  when $\mathbf{u}, \mathbf{u}_0, \mathbf{u}_1$ and basis $\mathbf{B}_1, \mathbf{B}_2$ are chosen at random. Here we use the fact that randomness $\mathbf{d}$ in secret keys reveals no information about the basis of $\mathsf{span}(\mathbf{B}_1, \mathbf{B}_2)$. See Lemma 5 for more details.
- Game_4 is identical to Game_3 except that the challenge ciphertext is

$$\boxed{x_{1,0} \cdot \mathbf{u}_0 + x_{1,1} \cdot \mathbf{u}_1} + \mathbf{w}_1,\ \ldots,\ \boxed{x_{n,0} \cdot \mathbf{u}_0 + x_{n,1} \cdot \mathbf{u}_1} + \mathbf{w}_n,\ [\alpha]_2 \cdot m_0$$

  in which the adversary has no advantage in guessing b. We claim that $\mathsf{Game}_3 \equiv \mathsf{Game}_4$. The proof is similar to that for $\mathsf{Game}_1 \equiv \mathsf{Game}_0$. See Lemma 6 for more details.

Proving $\mathsf{Game}_{2.j-1} \approx_c \mathsf{Game}_{2.j}$. We now prove $\mathsf{Game}_{2.j-1} \approx_c \mathsf{Game}_{2.j}$ and thus complete the proof for Lemma 2. For all $j \in [q]$, we employ the following game sequence, which has been included in Fig 3.

– $\mathsf{Game}_{2.j-1.1}$ is identical to $\mathsf{Game}_{2.j-1}$ except that the jth secret key is

$$[\alpha+(y_1\cdot\mathbf{w}_1+\cdots+y_n\cdot\mathbf{w}_n)\mathbf{d}]_2,\ [\mathbf{d}]_2 \quad \text{where} \quad \boxed{\mathbf{d}\leftarrow\mathsf{span}(\mathbf{B}_1,\mathbf{B}_3)}.$$

We claim that $\mathsf{Game}_{2.j-1.1}\approx_c \mathsf{Game}_{2.j-1}$. This follows from the $\mathrm{SD}^{G_2}_{\mathbf{B}_1\mapsto\mathbf{B}_1,\mathbf{B}_3}$ assumption stating that

$$[\mathbf{t}\leftarrow\mathsf{span}(\mathbf{B}_1)]_2\approx_c[\mathbf{t}\leftarrow\mathsf{span}(\mathbf{B}_1,\mathbf{B}_3)]_2 \quad \text{given} \quad [\mathbf{B}_1]_2,[\mathbf{B}_2]_2,[\mathbf{B}_3]_2,\mathsf{basis}(\mathbf{B}_2^{\|}),\mathsf{basis}(\mathbf{B}_1^{\|},\mathbf{B}_3^{\|}).$$

In the reduction, we sample $\alpha\leftarrow\mathbb{Z}_p$, $\mathbf{w}_1,\ldots,\mathbf{w}_n\leftarrow\mathbb{Z}_p^{1\times(2k+1)}$ and pick

$$\mathbf{u}^{(13)}\leftarrow\mathsf{span}((\mathbf{B}_1^{\|}|\mathbf{B}_3^{\|})^\top) \quad \text{and} \quad \mathbf{u}^{(2)}\leftarrow\mathsf{span}(\mathbf{B}_2^{\|\top})$$

using $\mathsf{basis}(\mathbf{B}_1^{\|},\mathbf{B}_3^{\|})$ and $\mathsf{basis}(\mathbf{B}_2^{\|})$, respectively. The challenge ciphertext is generated using

$$\{x_{i,b}\cdot\mathbf{u}^{(13)}+x_{i,1-b}\cdot\mathbf{u}^{(2)}+\mathbf{w}_i\}_{i\in[n]};$$

the jth secret key is created from $\mathbf{w}_1,\ldots,\mathbf{w}_n$ and $[\mathbf{t}]_2$ while the remaining keys can be generated using $[\mathbf{B}_1]_2$ and $[\mathbf{B}_2]_2$ along with $\alpha,\mathbf{w}_1,\ldots,\mathbf{w}_n$. See Lemma 7 for more details.

– $\mathsf{Game}_{2.j-1.2}$ is identical to $\mathsf{Game}_{2.j-1.1}$ except that the challenge ciphertext is

$$x_{1,b}\cdot\mathbf{u}^{(1)}+x_{1,1-b}\cdot\mathbf{u}^{(2)}+\boxed{x_{1,1-b}\cdot\mathbf{u}^{(3)}}+\mathbf{w}_1,\ \ldots,\ x_{n,b}\cdot\mathbf{u}^{(1)}+x_{n,1-b}\cdot\mathbf{u}^{(2)}+\boxed{x_{n,1-b}\cdot\mathbf{u}^{(3)}}+\mathbf{w}_n,\ [\alpha]_2\cdot m_0.$$

We claim that $\mathsf{Game}_{2.j-1.2}\equiv\mathsf{Game}_{2.j-1.1}$. This follows from facts that: (1) $\mathbf{u}^{(3)}$ and $\mathbf{w}_i^{(3)}$ are only revealed from the challenge ciphertext and the jth secret key; (2) for all $\mathbf{x}_0$, $\mathbf{x}_1$ and $\mathbf{y}$ with the restriction that (a) $\langle\mathbf{x}_0,\mathbf{y}\rangle=\langle\mathbf{x}_1,\mathbf{y}\rangle=0$; or (b) $\langle\mathbf{x}_0,\mathbf{y}\rangle\neq0\wedge\langle\mathbf{x}_1,\mathbf{y}\rangle\neq0$, it holds that

$$\begin{aligned}&(\overbrace{x_{1,b}\cdot\mathbf{u}^{(3)}+\mathbf{w}_1^{(3)},\ldots,x_{n,b}\cdot\mathbf{u}^{(3)}+\mathbf{w}_n^{(3)}}^{\mathsf{ct}},\ \overbrace{y_1\cdot\mathbf{w}_1^{(3)}+\cdots+y_n\cdot\mathbf{w}_n^{(3)}}^{\mathsf{sk}})\\ \equiv\ &(\boxed{x_{1,1-b}\cdot\mathbf{u}^{(3)}}+\mathbf{w}_1^{(3)},\ldots,\boxed{x_{n,1-b}\cdot\mathbf{u}^{(3)}}+\mathbf{w}_n^{(3)},\ y_1\cdot\mathbf{w}_1^{(3)}+\cdots+y_n\cdot\mathbf{w}_n^{(3)}).\end{aligned}$$

See Lemma 8 for more details.

– $\mathsf{Game}_{2.j-1.3}$ is identical to $\mathsf{Game}_{2.j-1.2}$ except that the jth secret key is

$$[\alpha+(y_1\cdot\mathbf{w}_1+\cdots+y_n\cdot\mathbf{w}_n)\mathbf{d}]_2,\ [\mathbf{d}]_2 \quad \text{where} \quad \boxed{\mathbf{d}\leftarrow\mathsf{span}(\mathbf{B}_1,\mathbf{B}_2,\mathbf{B}_3)}.$$

We claim that $\mathsf{Game}_{2.j-1.3}\approx_c\mathsf{Game}_{2.j-1.2}$. This follows from the $\mathrm{SD}^{G_2}_{\mathbf{B}_3\mapsto\mathbf{B}_3,\mathbf{B}_2}$ assumption stating that

$$[\mathbf{t}\leftarrow\mathsf{span}(\mathbf{B}_3)]_2\approx_c[\mathbf{t}\leftarrow\mathsf{span}(\mathbf{B}_2,\mathbf{B}_3)]_2 \quad \text{given} \quad [\mathbf{B}_1]_2,[\mathbf{B}_2]_2,[\mathbf{B}_3]_2,\mathsf{basis}(\mathbf{B}_1^{\|}),\mathsf{basis}(\mathbf{B}_2^{\|},\mathbf{B}_3^{\|}).$$

In the reduction, we sample $\alpha\leftarrow\mathbb{Z}_p$, $\mathbf{w}_1,\ldots,\mathbf{w}_n\leftarrow\mathbb{Z}_p^{1\times(2k+1)}$ and pick

$$\mathbf{u}^{(1)}\leftarrow\mathsf{span}(\mathbf{B}_1^{\|\top}) \quad \text{and} \quad \mathbf{u}^{(23)}\leftarrow\mathsf{span}((\mathbf{B}_2^{\|}|\mathbf{B}_3^{\|})^\top)$$

using $\mathsf{basis}(\mathbf{B}_1^{\|})$ and $\mathsf{basis}(\mathbf{B}_2^{\|},\mathbf{B}_3^{\|})$, respectively. The challenge ciphertext is generated using

$$\{x_{i,b}\cdot\mathbf{u}^{(1)}+x_{i,1-b}\cdot\mathbf{u}^{(23)}+\mathbf{w}_i\}_{i\in[n]}$$

the jth secret key is created from $\alpha,\mathbf{w}_1,\ldots,\mathbf{w}_n$ and $[\mathbf{B}_1]$, $[\mathbf{t}]_2$ while the remaining keys can be generated using $[\mathbf{B}_1,\mathbf{B}_2]_2$ along with $\alpha,\mathbf{w}_1,\ldots,\mathbf{w}_n$. See Lemma 9 for more details.

– $\mathsf{Game}_{2.j-1.4}$ is identical to $\mathsf{Game}_{2.j-1.3}$ except that the challenge ciphertext is

$$x_{1,b}\cdot\mathbf{u}^{(1)}+x_{1,1-b}\cdot\mathbf{u}^{(2)}+\boxed{x_{1,b}\cdot\mathbf{u}^{(3)}}+\mathbf{w}_1,\ \ldots,\ x_{n,b}\cdot\mathbf{u}^{(1)}+x_{n,1-b}\cdot\mathbf{u}^{(2)}+\boxed{x_{n,b}\cdot\mathbf{u}^{(3)}}+\mathbf{w}_n,\ [\alpha]_2\cdot m_0.$$

We claim that $\mathsf{Game}_{2.j-1.4}\equiv\mathsf{Game}_{2.j-1.3}$. The proof is identical to that for $\mathsf{Game}_{2.j-1.2}\equiv\mathsf{Game}_{2.j-1.1}$. See Lemma 10 for more details.

– $\mathsf{Game}_{2.j-1.5}$ is identical to $\mathsf{Game}_{2.j-1.4}$ except that the jth secret key is

$$[\alpha + (y_1 \cdot \mathbf{w}_1 + \cdots + y_n \cdot \mathbf{w}_n)\mathbf{d}]_2,\ [\mathbf{d}]_2 \quad \text{where} \quad \boxed{\mathbf{d} \leftarrow \mathsf{span}(\mathbf{B}_1, \mathbf{B}_2)}.$$

We claim that $\mathsf{Game}_{2.j-1.5} \approx_c \mathsf{Game}_{2.j-1.4}$. The proof is identical to that for $\mathsf{Game}_{2.j-1} \approx_c \mathsf{Game}_{2.j-1.1}$. See Lemma 11 for more details. Note that $\mathsf{Game}_{2.j-1.5} = \mathsf{Game}_{2.j}$.

3.4 Step Two: From private-key to public-key

We describe our prime-order full-fledged IPE, which is derived from our private-key IPE in Section 3.2 via the "private-key to public-key" compiler [36].

– $\mathsf{Setup}(1^\lambda, n)$: Run $\mathbb{G} = (p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}(1^\lambda)$. Sample $\mathbf{A} \leftarrow \mathbb{Z}_p^{(k+1)\times k}$, $\mathbf{B}_1 \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$ and pick

$$\mathbf{U}, \mathbf{W}_1, \ldots, \mathbf{W}_n \leftarrow \mathbb{Z}_p^{(k+1)\times(2k+1)} \quad \text{and} \quad \mathbf{k} \leftarrow \mathbb{Z}_p^{k+1}.$$

Output

$$\mathsf{mpk} = (\mathbb{G}, [\mathbf{A}^\top]_1, [\mathbf{A}^\top\mathbf{U}]_1, [\mathbf{A}^\top\mathbf{W}_1]_1, \ldots, [\mathbf{A}^\top\mathbf{W}_n]_1, [\mathbf{A}^\top\mathbf{k}]_T) \quad \text{and} \quad \mathsf{msk} = (\mathbf{k}, \mathbf{W}_1, \ldots, \mathbf{W}_n, \mathbf{B}_1).$$

– $\mathsf{KeyGen}(\mathsf{msk}, \mathbf{y})$: Let $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{Z}_p^n$. Sample $\mathbf{r} \leftarrow \mathbb{Z}_p^k$ and output

$$\mathsf{sk}_\mathbf{y} = (K_0 = [\mathbf{k} + (y_1 \cdot \mathbf{W}_1 + \cdots + y_n \cdot \mathbf{W}_n)\mathbf{B}_1\mathbf{r}]_2, K_1 = [\mathbf{B}_1\mathbf{r}]_2)$$

– $\mathsf{Enc}(\mathsf{mpk}, \mathbf{x}, m)$: Let $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}_p^n$ and $m \in G_T$. Sample $\mathbf{s} \leftarrow \mathbb{Z}_p^k$ and output

$$\mathsf{ct}_\mathbf{x} = (C_0 = [\mathbf{s}^\top\mathbf{A}^\top]_1, \{C_i = [\mathbf{s}^\top\mathbf{A}^\top(x_i \cdot \mathbf{U} + \mathbf{W}_i)]_1\}_{i\in[n]}, C = [\mathbf{s}^\top\mathbf{A}^\top\mathbf{k}]_T \cdot m)$$

– $\mathsf{Dec}(\mathsf{ct}_\mathbf{x}, \mathsf{sk}_\mathbf{y})$: Parse $\mathsf{ct}_\mathbf{x} = (C_0, C_1, \ldots, C_n, C)$ and $\mathsf{sk}_\mathbf{y} = (K_0, K_1)$ for $\mathbf{y} = (y_1, \ldots, y_n)$. Output

$$m' = C \cdot e(y_1 \odot C_1 \cdots y_n \odot C_n, K_1) \cdot e(C_0, K_0)^{-1}.$$

Correctness. For all $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_p^n$ with $\langle \mathbf{x}, \mathbf{y} \rangle = 0$, we have

$$\begin{aligned}
& e(y_1 \odot C_1 \cdots y_n \odot C_n, K_1) \cdot e(C_0, K_0)^{-1} \\
=\ & e([y_1 \cdot \mathbf{s}^\top\mathbf{A}^\top(x_1 \cdot \mathbf{U} + \mathbf{W}_1)]_1 \cdots [y_n \cdot \mathbf{s}^\top\mathbf{A}^\top(x_n \cdot \mathbf{U} + \mathbf{W}_n)]_1, [\mathbf{B}_1\mathbf{r}]_2) \cdot e([\mathbf{s}^\top\mathbf{A}_1^\top]_1, [\mathbf{k} + (y_1 \cdot \mathbf{W}_1 + \cdots + y_n \cdot \mathbf{W}_n)\mathbf{B}_1\mathbf{r}]_2)^{-1} \\
=\ & [\langle \mathbf{x}, \mathbf{y} \rangle \cdot \mathbf{s}^\top\mathbf{A}^\top\mathbf{U}\mathbf{B}_1\mathbf{r}]_T \cdot [\mathbf{s}^\top\mathbf{A}^\top(y_1 \cdot \mathbf{W}_1 + \cdots + y_n \cdot \mathbf{W}_n)\mathbf{B}_1\mathbf{r}]_T \cdot [\mathbf{s}^\top\mathbf{A}^\top\mathbf{k}]_T^{-1} \cdot [\mathbf{s}^\top\mathbf{A}^\top(y_1 \cdot \mathbf{W}_1 + \cdots + y_n \cdot \mathbf{W}_n)\mathbf{B}_1\mathbf{r}]_T^{-1} \\
=\ & [\mathbf{s}^\top\mathbf{A}^\top\mathbf{k}]_T^{-1}
\end{aligned}$$

where the last equality follows from the fact that $\langle \mathbf{x}, \mathbf{y} \rangle = 0$. This readily proves the correctness.

Security. We will prove the following theorem.

Theorem 2. *Under the k-LIN assumption, the IPE scheme described above is adaptively secure and fully attribute-hiding (cf. Section 2.1).*

For the same reason as in Section 3.3, we prove the lemma for the $m_0 = m_1$, which shows that the security of the IPE described above is implied by that of our private-key IPE in Section 3.2 and the MDDH_k assumption.

Lemma 3. *For any adversary $\mathcal{A}$ that makes at most Q key queries and outputs $m_0 = m_1$, there exists adversaries $\mathcal{B}_0, \mathcal{B}$ such that*

$$\mathsf{Adv}_\mathcal{A}^{\text{IPE}}(\lambda) \le \mathsf{Adv}_{\mathcal{B}_0}^{\text{MDDH}_k}(\lambda) + \mathsf{Adv}_\mathcal{B}^{\text{IPE}^*}(\lambda)$$

and $\mathsf{Time}(\mathcal{B}_0), \mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$.

We prove Lemma 3 via the following game sequence.

- Game_0 is the real game in which the challenge ciphertext for $\mathbf{x}_b = (x_{1,b}, \ldots, x_{n,b})$ is of the form
$$[\mathbf{c}^\top]_1, [\mathbf{c}^\top(x_{1,b}\cdot\mathbf{U}+\mathbf{W}_1)]_1, \ldots, [\mathbf{c}^\top(x_{n,b}\cdot\mathbf{U}+\mathbf{W}_n)]_1, e([\mathbf{c}^\top]_1, [\mathbf{k}]_2)\cdot m_0 \quad \text{where} \quad \mathbf{c}\leftarrow\mathsf{span}(\mathbf{A}).$$
Here $b \leftarrow \{0,1\}$ is a secret bit.
- Game_1 is identical to Game_0 except that we pick $\mathbf{c}\leftarrow\mathbb{Z}_p^{k+1}$ when generating the challenge ciphertext. We claim that $\mathsf{Game}_1 \approx_c \mathsf{Game}_0$. This follows from the MDDH_k assumption:
$$[\mathbf{c}\leftarrow\mathsf{span}(\mathbf{A})]_1 \approx_c [\mathbf{c}\leftarrow\mathbb{Z}_p^{k+1}] \quad \text{given} \quad [\mathbf{A}]_1.$$
In the reduction, we sample $\mathbf{k}, \mathbf{U}, \mathbf{W}_1, \ldots, \mathbf{W}_n$ and $\mathbf{B}_1$. The master public key mpk and the challenge ciphertext are simulated using $\mathbf{k}, \mathbf{U}, \mathbf{W}_1, \ldots, \mathbf{W}_n$ along with $[\mathbf{A}]_1$, $[\mathbf{c}]_1$; all secret keys can be created honestly. See Lemma 12 for more details.

It remains to show that the advantage in guessing $b\in\{0,1\}$ in Game_1 is negligible. This follows from the security of our private-key IPE in Section 3.2. For $\mathbf{A}$ and $\mathbf{c}$, define

$$\begin{array}{lll} \mathbf{A}^\top\mathbf{U} = \widetilde{\mathbf{U}} \in \mathbb{Z}_p^{k\times(2k+1)} & \mathbf{A}^\top\mathbf{W}_i = \widetilde{\mathbf{W}}_i \in \mathbb{Z}_p^{k\times(2k+1)} & \mathbf{A}^\top\mathbf{k} = \widetilde{\mathbf{k}} \in \mathbb{Z}_p^{k} \\ \mathbf{c}^\top\mathbf{U} = \mathbf{u} \in \mathbb{Z}_p^{1\times(2k+1)} & \mathbf{c}^\top\mathbf{W}_i = \mathbf{w}_i \in \mathbb{Z}_p^{1\times(2k+1)} & \mathbf{c}^\top\mathbf{k} = \alpha \in \mathbb{Z}_p \end{array}$$

We can then rewrite mpk as
$$[\mathbf{A}^\top]_1, [\widetilde{\mathbf{U}}]_1, [\widetilde{\mathbf{W}}_1]_1, \ldots, [\widetilde{\mathbf{W}}_n]_1, [\widetilde{\mathbf{k}}]_T;$$
the challenge ciphertext (in Game_1) becomes
$$[\mathbf{c}^\top]_1, [\underline{x_{1,b}\cdot\mathbf{u}+\mathbf{w}_1}]_1, \ldots, [\underline{x_{n,b}\cdot\mathbf{u}+\mathbf{w}_n}]_1, e([1]_1, \underline{[\alpha]_2})\cdot m_0.$$
Assume that $(\mathbf{A}|\mathbf{c})$ is full-rank which occurs with high probability and define $\mathbf{T} = \binom{\mathbf{A}^\top}{\mathbf{c}^\top}^{-1}$, we have $\mathbf{W}_i = \mathbf{T}\binom{\widetilde{\mathbf{W}}_i}{\mathbf{w}_i}$ and $\mathbf{k} = \mathbf{T}\binom{\widetilde{\mathbf{k}}}{\alpha}$, a secret key can be rewritten as
$$\mathbf{T}\odot\begin{pmatrix} [\widetilde{\mathbf{k}} + (y_1\cdot\widetilde{\mathbf{W}}_1 + \cdots + y_n\cdot\widetilde{\mathbf{W}}_n)\mathbf{d}]_2 \\ \underline{[\alpha + (y_1\cdot\mathbf{w}_1 + \cdots + y_n\cdot\mathbf{w}_n)\mathbf{d}]_2} \end{pmatrix}, \underline{[\mathbf{d}]_2}.$$
Observe that the underlined parts are *exactly* the ciphertext and secret keys of our private-key IPE in Section 3.2; and $(\widetilde{\mathbf{U}}, \widetilde{\mathbf{W}}_i, \widetilde{\mathbf{k}})$, $(\mathbf{u}, \mathbf{w}_i, \alpha)$ are distributed uniformly and *independently*. This means we can simulate mpk honestly and transform a ciphertext/secret key from our private-key IPE to its public-key counterpart using $\mathbf{A}$, $\mathbf{c}$, $\widetilde{\mathbf{U}}$, $\widetilde{\mathbf{W}}_i$, $\widetilde{\mathbf{k}}$. This is sufficient for the reduction from the public-key IPE to private-key IPE. See Lemma 13 for more details.

3.5 Lemmas for Private-key IPE

Let Adv_x be the advantage function with respect to $\mathcal{A}$ in Game_x. We prove the following lemma for the game sequence in Section 3.3.

Lemma 4 ($\mathsf{Game}_0 \equiv \mathsf{Game}_1$)**.** $\mathsf{Adv}_0(\lambda) = \mathsf{Adv}_1(\lambda)$.

Proof. It is sufficient to prove that, for all $\mathbf{u}\leftarrow\mathbb{Z}_p^{1\times(2k+1)}$, it holds that
$$\begin{aligned} &(\overbrace{\mathbf{w}_1\mathbf{B}_1, \ldots, \mathbf{w}_n\mathbf{B}_1}^{\mathsf{sk}}, \overbrace{x_{1,b}\cdot\mathbf{u}^{(13)} + \boxed{x_{1,b}}\cdot\mathbf{u}^{(2)} + \mathbf{w}_1, \cdots, x_{n,b}\cdot\mathbf{u}^{(13)} + \boxed{x_{n,b}}\cdot\mathbf{u}^{(2)} + \mathbf{w}_n}^{\mathsf{ct}}) \\ \equiv\ &(\mathbf{w}_1\mathbf{B}_1, \ldots, \mathbf{w}_n\mathbf{B}_1, x_{1,b}\cdot\mathbf{u}^{(13)} + \boxed{x_{1,1-b}}\cdot\mathbf{u}^{(2)} + \mathbf{w}_1, \cdots, x_{n,b}\cdot\mathbf{u}^{(13)} + \boxed{x_{n,1-b}}\cdot\mathbf{u}^{(2)} + \mathbf{w}_n) \end{aligned}$$

when $\mathbf{w}_1, \ldots, \mathbf{w}_n \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$. By the facts shown in Section 3.1, it is implied by the statement that, for all $\mathbf{u}^{(2)} \in \mathsf{span}(\mathbf{B}_2^{\|\top})$, it holds that

$$\{x_{i,b} \cdot \mathbf{u}^{(2)} + \mathbf{w}_i^{(2)}\}_{i\in[n]} \equiv \{\mathbf{w}_i^{(2)}\}_{i\in[n]} \equiv \{x_{i,1-b} \cdot \mathbf{u}^{(2)} + \mathbf{w}_i^{(2)}\}_{i\in[n]}$$

when $\mathbf{w}_1^{(2)}, \ldots, \mathbf{w}_n^{(2)} \leftarrow \mathsf{span}(\mathbf{B}_2^{\|\top})$. This completes the proof. □

Lemma 5 ($\mathsf{Game}_{2.q} \equiv \mathsf{Game}_3$)**.** $\mathsf{Adv}_{2.q}(\lambda) = \mathsf{Adv}_3(\lambda)$.

Proof. We simulate $\mathsf{Game}_{2.q}$ as follows:

Setup. We alternatively prepare basis $(\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3)$ as follows: Sample $\widetilde{\mathbf{B}}_1, \mathbf{B}_3 \leftarrow \mathbb{Z}_p^{(2k+1)\times k}, \widetilde{\mathbf{B}}_2 \leftarrow \mathbb{Z}_p^{2k+1}$ and compute dual basis $\widetilde{\mathbf{B}}_1^{\|}, \widetilde{\mathbf{B}}_2^{\|}, \mathbf{B}_3^{\|}$ as usual. Pick $\mathbf{R} \leftarrow \mathrm{GL}_{k+1}(\mathbb{Z}_p)$ and define

$$(\mathbf{B}_1|\mathbf{B}_2) = (\widetilde{\mathbf{B}}_1|\widetilde{\mathbf{B}}_2)\mathbf{R} \quad \text{and} \quad (\mathbf{B}_1^{\|}|\mathbf{B}_2^{\|}) = (\widetilde{\mathbf{B}}_1^{\|}|\widetilde{\mathbf{B}}_2^{\|})\mathbf{R}^*.$$

This does not change the distribution of basis. We then sample $\alpha, \mathbf{u}, \mathbf{w}_1, \ldots, \mathbf{w}_n$ honestly.

Key queries. On input $\mathbf{y} = (y_1, \ldots, y_n)$, output

$$[\alpha + (y_1 \cdot \mathbf{w}_1 + \cdots + y_n \cdot \mathbf{w}_n)\mathbf{d}]_2,\ [\mathbf{d}]_2 \quad \text{where} \quad \mathbf{d} \leftarrow \mathsf{span}(\widetilde{\mathbf{B}}_1, \widetilde{\mathbf{B}}_2).$$

Although we sample $\mathbf{d}$ using $\widetilde{\mathbf{B}}_1, \widetilde{\mathbf{B}}_2$, the vector is uniformly distributed over $\mathsf{span}(\mathbf{B}_1, \mathbf{B}_2)$ as required and our simulation is perfect.

Ciphertext. On input $(\mathbf{x}_0, \mathbf{x}_1, m_0, m_1)$ with $m_0 = m_1$, we create the challenge ciphertext honestly using $(\mathbf{B}_1^{\|}, \mathbf{B}_2^{\|}, \mathbf{B}_3^{\|})$. That is, we pick $b \leftarrow \{0,1\}$ and output

$$x_{1,b} \cdot \mathbf{v}_0 + x_{1,1-b} \cdot \mathbf{v}_1 + x_{1,b} \cdot \mathbf{u}^{(3)} + \mathbf{w}_1, \ldots, x_{n,b} \cdot \mathbf{v}_0 + x_{n,1-b} \cdot \mathbf{v}_1 + x_{n,b} \cdot \mathbf{u}^{(3)} + \mathbf{w}_n,\ [\alpha]_2 \cdot m_0$$

where $\mathbf{u}^{(3)} \leftarrow \mathsf{span}(\mathbf{B}_3^{\|\top})$ and

$$\mathbf{v}_0 = \mathbf{u}^{(1)} \leftarrow \mathsf{span}(\mathbf{B}_1^{\|\top}) \quad \text{and} \quad \mathbf{v}_1 = \mathbf{u}^{(2)} \leftarrow \mathsf{span}(\mathbf{B}_2^{\|\top}).$$

Observe that, we have a 2-by-$(k+1)$ matrix $\mathbf{V}$ of rank 2 such that

$$\begin{pmatrix} —\mathbf{v}_0— \\ —\mathbf{v}_1— \end{pmatrix} = \mathbf{V}(\mathbf{B}_1^{\|}|\mathbf{B}_2^{\|})^\top = \underbrace{\mathbf{V}\mathbf{R}^{-1}}_{\text{uniformly over } \mathbb{Z}_p^{2\times(k+1)}} (\widetilde{\mathbf{B}}_1^{\|}|\widetilde{\mathbf{B}}_2^{\|})^\top.$$

Since $\mathbf{R}$ is independent of other part of simulation, $\mathbf{V}\mathbf{R}^{-1}$ are uniformly distributed over $\mathbb{Z}_p^{2\times(k+1)}$ and thus it is equivalent to sample $\mathbf{v}_0, \mathbf{v}_1 \leftarrow \mathsf{span}((\widetilde{\mathbf{B}}_1^{\|}|\widetilde{\mathbf{B}}_2^{\|})^\top)$ when creating the challenge ciphertext. This leads to the simulation of Game_3 (with respect to $\widetilde{\mathbf{B}}_1, \widetilde{\mathbf{B}}_2, \mathbf{B}_3$). □

Lemma 6 ($\mathsf{Game}_3 \equiv \mathsf{Game}_4$)**.** $\mathsf{Adv}_3(\lambda) = \mathsf{Adv}_4(\lambda)$.

Proof. The proof is similar to that for Lemma 4, except that we work with $\mathbf{u}^{(3)}, \mathbf{u}_0^{(3)}, \mathbf{u}_1^{(3)}, \mathbf{w}_i^{(3)}$ instead. □

Lemma 7 ($\mathsf{Game}_{2.j-1} \approx_c \mathsf{Game}_{2.j-1.1}$)**.** *There exists adversary* $\mathcal{B}_1$ *with* $\mathsf{Time}(\mathcal{B}_1) \approx \mathsf{Time}(\mathcal{A})$ *such that*

$$|\mathsf{Adv}_{2.j-1.1}(\lambda) - \mathsf{Adv}_{2.j-1}(\lambda)| \le \mathsf{Adv}_{\mathcal{B}_1}^{\mathrm{SD}^{G_2}_{\mathbf{B}_1 \mapsto \mathbf{B}_1,\mathbf{B}_3}}(\lambda).$$

Proof. This follows from the $\mathrm{SD}^{G_2}_{\mathbf{B}_1 \mapsto \mathbf{B}_1,\mathbf{B}_3}$ assumption stating that

$$[\mathbf{t} \leftarrow \mathsf{span}(\mathbf{B}_1)]_2 \approx_c [\mathbf{t} \leftarrow \mathsf{span}(\mathbf{B}_1, \mathbf{B}_3)]_2 \quad \text{given} \quad [\mathbf{B}_1]_2, [\mathbf{B}_2]_2, [\mathbf{B}_3]_2, \mathsf{basis}(\mathbf{B}_2^{\|}), \mathsf{basis}(\mathbf{B}_1^{\|}, \mathbf{B}_3^{\|}).$$

On input $[\mathbf{B}_1]_2, [\mathbf{B}_2]_2, [\mathbf{B}_3]_2, \mathsf{basis}(\mathbf{B}_2^{\|}), \mathsf{basis}(\mathbf{B}_1^{\|}, \mathbf{B}_3^{\|})$ and $[\mathbf{t}]_2$, the adversary $\mathcal{B}_1$ works as follows:

Setup. Sample $\alpha \leftarrow \mathbb{Z}_p$, $\mathbf{w}_1, \ldots, \mathbf{w}_n \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$. Implicitly sample $\mathbf{u}$ by picking

$$\mathbf{u}^{(13)} \leftarrow \mathsf{span}((\mathbf{B}_1^{\|}|\mathbf{B}_3^{\|})^\top) \quad \text{and} \quad \mathbf{u}^{(2)} \leftarrow \mathsf{span}(\mathbf{B}_2^{\|}{}^\top)$$

using $\mathsf{basis}(\mathbf{B}_1^{\|}, \mathbf{B}_3^{\|})$ and $\mathsf{basis}(\mathbf{B}_2^{\|})$, respectively.

Key Queries. On the κth query $\mathbf{y} = (y_1, \ldots, y_n)$, output

$$[\alpha + (y_1 \cdot \mathbf{w}_1 + \cdots + y_n \cdot \mathbf{w}_n)\mathbf{d}]_2, [\mathbf{d}]_2 \quad \text{where} \quad \mathbf{d} \leftarrow \begin{cases} \mathsf{span}(\mathbf{B}_1, \mathbf{B}_2) & \kappa < j; \\ \mathbf{t} & \kappa = j; \\ \mathsf{span}(\mathbf{B}_1) & \kappa > j; \end{cases}$$

using $[\mathbf{B}_1]_2$, $[\mathbf{B}_2]_2$ and $[\mathbf{t}]_2$

Ciphertext. On input $(\mathbf{x}_0, \mathbf{x}_1, m_0, m_1)$ with $m_0 = m_1$, pick $b \leftarrow \{0,1\}$ and output

$$x_{1,b} \cdot \mathbf{u}^{(13)} + x_{1,1-b} \cdot \mathbf{u}^{(2)} + \mathbf{w}_1, \ldots, x_{n,b} \cdot \mathbf{u}^{(13)} + x_{n,1-b} \cdot \mathbf{u}^{(2)} + \mathbf{w}_n, [\alpha]_2 \cdot m_0.$$

Observe that, when $\mathbf{t}$ is uniformly distributed over $\mathsf{span}(\mathbf{B}_1)$, the simulation is identical to $\mathsf{Game}_{2.j-1}$; otherwise, when $\mathbf{t}$ is uniformly distributed over $\mathsf{span}(\mathbf{B}_1, \mathbf{B}_3)$, the simulation is identical to $\mathsf{Game}_{2.j-1.1}$. This proves the lemma. □

Lemma 8 ($\mathsf{Game}_{2.j-1.1} \equiv \mathsf{Game}_{2.j-1.2}$)**.** $\mathsf{Adv}_{2.j-1.1} = \mathsf{Adv}_{2.j-1.2}$.

Proof. By complexity leveraging and the facts shown in Section 3.1, it is sufficient to prove the following statement: for all $\mathbf{x}_0$, $\mathbf{x}_1$ and $\mathbf{y}$ (corresponding to the jth key query) satisfying that (a) $\langle \mathbf{x}_0, \mathbf{y}\rangle = \langle \mathbf{x}_1, \mathbf{y}\rangle = 0$; or (b) $\langle \mathbf{x}_0, \mathbf{y}\rangle \neq 0 \wedge \langle \mathbf{x}_1, \mathbf{y}\rangle \neq 0$, it holds that

$$\begin{aligned} &(\overbrace{x_{1,b} \cdot \mathbf{u}^{(3)} + \mathbf{w}_1^{(3)}, \ldots, x_{n,b} \cdot \mathbf{u}^{(3)} + \mathbf{w}_n^{(3)}}^{\mathsf{ct}}, \overbrace{y_1 \cdot \mathbf{w}_1^{(3)} + \cdots + y_n \cdot \mathbf{w}_n^{(3)}}^{\mathsf{sk}}) \\ \equiv &(\boxed{x_{1,1-b}} \cdot \mathbf{u}^{(3)} + \mathbf{w}_1^{(3)}, \ldots, \boxed{x_{n,1-b}} \cdot \mathbf{u}^{(3)} + \mathbf{w}_n^{(3)}, y_1 \cdot \mathbf{w}_1^{(3)} + \cdots + y_n \cdot \mathbf{w}_n^{(3)}) \end{aligned}$$

when $\mathbf{u}^{(3)}, \mathbf{w}_1^{(3)}, \ldots, \mathbf{w}_n^{(3)} \leftarrow \mathsf{span}(\mathbf{B}_3^{\|}{}^\top)$. By the linearity, it in turn follows from the following statement

$$\begin{aligned} &\{x_{1,b} \cdot u + w_1, \ldots, x_{n,b} \cdot u + w_n,\ y_1 \cdot w_1 + \cdots + y_n \cdot w_n\} \\ \equiv &\{\boxed{x_{1,1-b}} \cdot u + w_1, \ldots, \boxed{x_{n,1-b}} \cdot u + w_n,\ y_1 \cdot w_1 + \cdots + y_n \cdot w_n\} \end{aligned}$$

where $u, w_1, \ldots, w_n \leftarrow \mathbb{Z}_p$. This follows from the statistical argument for all $\mathbf{x} = (x_1, \ldots, x_n)$ which is implicitly used in the proof of Wee's simulation-based selectively secure IPE [36]: by programming $\tilde{w}_i = x_i \cdot u + w_i$ for all $i \in [n]$, we have

$$\begin{aligned} &\{x_1 \cdot u + w_1, \ldots, x_n \cdot u + w_n,\ y_1 \cdot w_1 + \cdots + y_n \cdot w_n\} \\ \equiv &\{\tilde{w}_1, \ldots, \tilde{w}_n,\ (y_1 \cdot \tilde{w}_1 + \cdots + y_n \cdot \tilde{w}_n) - u \cdot (x_1 y_1 + \cdots + x_n y_n)\} \end{aligned}$$

which means that the left-hand side distributions for all vector $\mathbf{x}$ not orthogonal to $\mathbf{y}$ are identical (since u hides the information about the inner-product) and so do all vector $\mathbf{x}$ orthogonal to $\mathbf{y}$. This immediately proves the above statement and thus proves the lemma. □

Lemma 9 ($\mathsf{Game}_{2.j-1.2} \approx_c \mathsf{Game}_{2.j-1.3}$)**.** *There exists adversary* $\mathcal{B}_2$ *with* $\mathsf{Time}(\mathcal{B}_2) \approx \mathsf{Time}(\mathcal{A})$ *such that*

$$|\mathsf{Adv}_{2.j-1.3}(\lambda) - \mathsf{Adv}_{2.j-1.2}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_2}^{\mathrm{SD}^{G_2}_{\mathbf{B}_3 \mapsto \mathbf{B}_3, \mathbf{B}_2}}(\lambda).$$

Proof. This follows from the $\text{SD}^{G_2}_{\mathbf{B}_3 \mapsto \mathbf{B}_3,\mathbf{B}_2}$ assumption stating that

$$[\mathbf{t} \leftarrow \mathsf{span}(\mathbf{B}_3)]_2 \approx_c [\mathbf{t} \leftarrow \mathsf{span}(\mathbf{B}_2,\mathbf{B}_3)]_2 \quad \text{given} \quad [\mathbf{B}_1]_2, [\mathbf{B}_2]_2, [\mathbf{B}_3]_2, \mathsf{basis}(\mathbf{B}_1^{\|}), \mathsf{basis}(\mathbf{B}_2^{\|}, \mathbf{B}_3^{\|}).$$

On input $[\mathbf{B}_1]_2, [\mathbf{B}_2]_2, [\mathbf{B}_3]_2, \mathsf{basis}(\mathbf{B}_1^{\|}), \mathsf{basis}(\mathbf{B}_2^{\|}, \mathbf{B}_3^{\|})$ and $[\mathbf{t}]_2$, the adversary $\mathcal{B}_2$ works as follows:

Setup. Sample $\alpha \leftarrow \mathbb{Z}_p$, $\mathbf{w}_1, \ldots, \mathbf{w}_n \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$. Implicitly sample $\mathbf{u}$ by picking

$$\mathbf{u}^{(1)} \leftarrow \mathsf{span}(\mathbf{B}_1^{\|\top}) \quad \text{and} \quad \mathbf{u}^{(23)} \leftarrow \mathsf{span}((\mathbf{B}_2^{\|}|\mathbf{B}_3^{\|})^\top)$$

using $\mathsf{basis}(\mathbf{B}_1^{\|})$ and $\mathsf{basis}(\mathbf{B}_2^{\|}, \mathbf{B}_3^{\|})$, respectively.

Key Queries. On the κth query $\mathbf{y} = (y_1, \ldots, y_n)$, output

$$[\alpha + (y_1 \cdot \mathbf{w}_1 + \cdots + y_n \cdot \mathbf{w}_n)\mathbf{d}]_2, [\mathbf{d}]_2 \quad \text{where} \quad \mathbf{d} \leftarrow \begin{cases} \mathsf{span}(\mathbf{B}_1, \mathbf{B}_2) & \kappa < j; \\ \mathbf{t} + \mathsf{span}(\mathbf{B}_1) & \kappa = j; \\ \mathsf{span}(\mathbf{B}_1) & \kappa > j; \end{cases}$$

using $[\mathbf{B}_1]_2$, $[\mathbf{B}_2]_2$, and $[\mathbf{t}]_2$.

Ciphertext. On input $(\mathbf{x}_0, \mathbf{x}_1, m_0, m_1)$ with $m_0 = m_1$, pick $b \leftarrow \{0,1\}$ and output

$$x_{1,b} \cdot \mathbf{u}^{(1)} + x_{1,1-b} \cdot \mathbf{u}^{(23)} + \mathbf{w}_1, \ldots, x_{n,b} \cdot \mathbf{u}^{(1)} + x_{n,1-b} \cdot \mathbf{u}^{(23)} + \mathbf{w}_n, [\alpha]_2 \cdot m_0.$$

Observe that, when $\mathbf{t}$ is uniformly distributed over $\mathsf{span}(\mathbf{B}_3)$, the simulation is identical to $\mathsf{Game}_{2.j-1.2}$; otherwise, when $\mathbf{t}$ is uniformly distributed over $\mathsf{span}(\mathbf{B}_2, \mathbf{B}_3)$, the simulation is identical to $\mathsf{Game}_{2.j-1.3}$. This proves the lemma. □

Lemma 10 **(**$\mathsf{Game}_{2.j-1.3} \equiv \mathsf{Game}_{2.j-1.4}$**).** $\mathsf{Adv}_{2.j-1.3} = \mathsf{Adv}_{2.j-1.4}$.

Proof. The proof is identical to that for Lemma 8 ($\mathsf{Game}_{2.j-1.1} \approx_c \mathsf{Game}_{2.j-1.2}$). □

Lemma 11 **(**$\mathsf{Game}_{2.j-1.4} \approx_c \mathsf{Game}_{2.j-1.5}$**).** *There exists adversary* $\mathcal{B}_3$ *with* $\mathsf{Time}(\mathcal{B}_3) \approx \mathsf{Time}(\mathcal{A})$ *such that*

$$|\mathsf{Adv}_{2.j-1.5}(\lambda) - \mathsf{Adv}_{2.j-1.4}(\lambda)| \le \mathsf{Adv}_{\mathcal{B}_3}^{\text{SD}^{G_2}_{\mathbf{B}_1 \mapsto \mathbf{B}_1,\mathbf{B}_3}}(\lambda).$$

Proof. The proof is analogous to that for Lemma 7 ($\mathsf{Game}_{2.j-1} \approx_c \mathsf{Game}_{2.j-1.1}$), except that: on the jth query $\mathbf{y} = (y_1, \ldots, y_n)$, we output

$$[\alpha + (y_1 \cdot \mathbf{w}_1 + \cdots + y_n \cdot \mathbf{w}_n)\mathbf{d}]_2, [\mathbf{d}]_2 \quad \text{where} \quad \boxed{\mathbf{d} \leftarrow \mathbf{t} + \mathsf{span}(\mathbf{B}_2)}.$$

using $[\mathbf{B}_2]_2$ and $[\mathbf{t}]_2$. □

3.6 Lemmas for Public-key IPE

Let Adv_x be the advantage function with respect to $\mathcal{A}$ in Game_x. We prove the following lemma for the game sequence in Section 3.4.

Lemma 12 **(**$\mathsf{Game}_0 \equiv \mathsf{Game}_1$**).** *There exists adversary* $\mathcal{B}_0$ *with* $\mathsf{Time}(\mathcal{B}_0) \approx \mathsf{Time}(\mathcal{A})$ *such that*

$$|\mathsf{Adv}_1(\lambda) - \mathsf{Adv}_0(\lambda)| \le \mathsf{Adv}_{\mathcal{B}_0}^{\text{MDDH}_k}(\lambda).$$

Proof. This follows from the MDDH_k assumption stating that

$$[\mathbf{c} \leftarrow \mathsf{span}(\mathbf{A})]_1 \approx_c [\mathbf{c} \leftarrow \mathbb{Z}_p^{k+1}] \quad \text{given} \quad [\mathbf{A}]_1.$$

On input $[\mathbf{A}]_1$ and $[\mathbf{c}]_1$, the adversary $\mathcal{B}_0$ works as follows:

Setup. Sample $\mathbf{k} \leftarrow \mathbb{Z}_p^{k+1}$, $\mathbf{U}, \mathbf{W}_1, \ldots, \mathbf{W} \leftarrow \mathbb{Z}_p^{(k+1)\times(2k+1)}$ and $\mathbf{B}_1 \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$. Output

$$([\mathbf{A}^\top]_1, [\mathbf{A}^\top\mathbf{U}]_1, [\mathbf{A}^\top\mathbf{W}_1]_1, \ldots, [\mathbf{A}^\top\mathbf{W}_n]_1, [\mathbf{A}^\top\mathbf{k}]_T)$$

using $[\mathbf{A}]_1$.

Key Queries. On query $\mathbf{y} = (y_1, \ldots, y_n)$, output

$$[\alpha + (y_1 \cdot \mathbf{w}_1 + \cdots + y_n \cdot \mathbf{w}_n)\mathbf{d}]_2, [\mathbf{d}]_2 \quad \text{where} \quad \mathbf{d} \leftarrow \mathsf{span}(\mathbf{B}_1).$$

Ciphertext. On input $(\mathbf{x}_0, \mathbf{x}_1, m_0, m_1)$ with $m_0 = m_1$, pick $b \leftarrow \{0,1\}$ and output

$$[\mathbf{c}^\top]_1, [\mathbf{c}^\top(x_{1,b} \cdot \mathbf{U} + \mathbf{W}_1)]_1, \ldots, [\mathbf{c}^\top(x_{n,b} \cdot \mathbf{U} + \mathbf{W}_n)]_1, e([\mathbf{c}^\top]_1, [\mathbf{k}]_2) \cdot m_0.$$

Observe that, when $\mathbf{c}$ is uniformly distributed over $\mathsf{span}(\mathbf{A})$, the simulation is identical to Game_0; otherwise, when $\mathbf{c}$ is uniformly distributed over $\mathbb{Z}_p^{k+1}$, the simulation is identical to Game_1. This proves the lemma. □

Lemma 13 **(Advantage in** Game_1**).** *There exists adversary* $\mathcal{B}$ *with* $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ *such that*

$$\mathsf{Adv}_1(\lambda) \leq \mathsf{Adv}_{\mathcal{B}}^{\mathrm{IPE}^*}(\lambda).$$

Proof. We construct the adversary $\mathcal{B}$ as below:

Setup. Sample $(\mathbf{A}, \mathbf{c}) \leftarrow \mathbb{Z}_p^{(k+1)\times k} \times \mathbb{Z}_p^{k+1}$ and compute $\mathbf{T} = \begin{pmatrix} \mathbf{A}^\top \\ \mathbf{c}^\top \end{pmatrix}^{-1}$. Since $(\mathbf{A}|\mathbf{c})$ is full-rank which occurs with high probability, $\mathbf{T}$ is well-defined. Pick

$$\widetilde{\mathbf{U}}, \widetilde{\mathbf{W}}_1, \ldots, \widetilde{\mathbf{W}}_n \leftarrow \mathbb{Z}_p^{k\times(2k+1)} \quad \text{and} \quad \widetilde{\mathbf{k}} \leftarrow \mathbb{Z}_p^k$$

and output

$$\mathsf{mpk} = ([\mathbf{A}^\top]_1, [\widetilde{\mathbf{U}}]_1, [\widetilde{\mathbf{W}}_1]_1, \ldots, [\widetilde{\mathbf{W}}_n]_1, [\widetilde{\mathbf{k}}]_T).$$

Key Queries. On input $\mathbf{y}$, adversary $\mathcal{B}$ forwards the query to its environment and receives (K_0, K_1). Compute

$$\widetilde{K}_0 = [\widetilde{\mathbf{k}}]_2 \cdot ((y_1 \cdot \widetilde{\mathbf{W}}_1 + \cdots + y_n \cdot \widetilde{\mathbf{W}}_n) \odot K_0)$$

and output

$$\mathsf{sk}_{\mathbf{y}} = \left(\mathbf{T} \odot \begin{pmatrix} \widetilde{K}_0 \\ K_0 \end{pmatrix}, \ K_1\right).$$

Ciphertext. On input $(\mathbf{x}_0, \mathbf{x}_1, m_0, m_1)$, adversary $\mathcal{B}$ sends query $(\mathbf{x}_0, \mathbf{x}_1, 1, 1)$ to its environment and receives $(C_1, \ldots, C_n, C)$. Create the challenge ciphertext as

$$[\mathbf{c}^\top]_1, [C_1]_1, \ldots, [C_n]_1, e([1]_1, C) \cdot m_0.$$

The adversary $\mathcal{B}$ outputs $\mathcal{A}$'s guess bit. By the observation in Section 3.4, mpk is simulated perfectly; if (K_0, K_1) is a private-key IPE secret key, secret keys we computed is for our public-key IPE; if $(C_1, \ldots, C_n, C)$ is a private-key IPE ciphertext for $b = 0$, the ciphertext we created is a public-key IPE ciphertext for $b = 0$; this also holds for $b = 1$. This readily proves the lemma. □

4 Construction from XDLIN assumption

In this section, we improve the IPE scheme presented in Section 3 by the optimization technique in [16]. As in Section 3, we will first develop a private-key IPE from that in Section 3.2 and then compile it into the public-key setting.

4.1 Correspondence

Applying the technique in [16] to our private-key IPE in Section 3.2, we basically overlap $\mathsf{span}(\mathbf{B}_1)$ and $\mathsf{span}(\mathbf{B}_3)$ so that the total dimension decreases. Technically, we work with basis

$$\mathbf{B}_1 \leftarrow \mathbb{Z}_p^{\ell\times\ell_1},\ \mathbf{B}_2 \leftarrow \mathbb{Z}_p^{\ell\times\ell_2},\ \mathbf{B}_3 \leftarrow \mathbb{Z}_p^{\ell\times\ell_3},\ \mathbf{B}_4 \leftarrow \mathbb{Z}_p^{\ell\times\ell_4}$$

where $\ell_1,\ell_2,\ell_3,\ell_4 \geq 1$ and $\ell := \ell_1+\ell_2+\ell_3+\ell_4$, and follow the correspondence:

$$\begin{array}{rcl} \text{Sec 3.1} & & \text{this section} \\ \mathbf{B}_1 & \mapsto & (\mathbf{B}_1 \mid \mathbf{B}_4) \\ \mathbf{B}_2 & \mapsto & \mathbf{B}_2 \\ \mathbf{B}_3 & \mapsto & (\mathbf{B}_3 \mid \mathbf{B}_4) \end{array} \tag{10}$$

saying that $\mathbf{B}_1$ and $\mathbf{B}_3$ used in Section 3 are replaced by $(\mathbf{B}_1|\mathbf{B}_4)$ and $(\mathbf{B}_3|\mathbf{B}_4)$, respectively, whose spans interact at $\mathsf{span}(\mathbf{B}_4)$. Analogous to Section 3.1, we can define its dual basis $(\mathbf{B}_1^\parallel,\mathbf{B}_2^\parallel,\mathbf{B}_3^\parallel,\mathbf{B}_4^\parallel)$ and decompose $\mathbf{w}\in\mathbb{Z}_p^{1\times\ell}$ as $\mathbf{w}^{(1)}+\mathbf{w}^{(2)}+\mathbf{w}^{(3)}+\mathbf{w}^{(4)}$.

Assumptions. With the correspondence (10), the assumption $\mathrm{SD}^{G_2}_{\mathbf{B}_1\mapsto\mathbf{B}_1,\mathbf{B}_3}$ used in Section 3.3 will be replaced by $\mathrm{SD}^{G_2}_{\mathbf{B}_1,\mathbf{B}_4\mapsto\mathbf{B}_1,\mathbf{B}_3,\mathbf{B}_4}$ defined as follows.

Lemma 14 ($\mathrm{MDDH}_{\ell_1+\ell_4,\ell_1+\ell_3+\ell_4} \Rightarrow \mathrm{SD}^{G_2}_{\mathbf{B}_1,\mathbf{B}_4\mapsto\mathbf{B}_1,\mathbf{B}_3,\mathbf{B}_4}$). *Under the $\mathrm{MDDH}_{\ell_1+\ell_4,\ell_1+\ell_3+\ell_4}$ assumption in G_2, there exists an efficient sampler outputting random* $([\mathbf{B}_1]_2,[\mathbf{B}_2]_2,[\mathbf{B}_3]_2,[\mathbf{B}_4]_2)$ *along with base* $\mathsf{basis}(\mathbf{B}_2^\parallel)$ *and* $\mathsf{basis}(\mathbf{B}_1^\parallel,\mathbf{B}_3^\parallel,\mathbf{B}_4^\parallel)$ *(of arbitrary choice) such that the following advantage function is negligible in λ.*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{SD}^{G_2}_{\mathbf{B}_1,\mathbf{B}_4\mapsto\mathbf{B}_1,\mathbf{B}_3,\mathbf{B}_4}}(\lambda) := |\Pr[\mathcal{A}(\mathbb{G},D,[\mathbf{t}_0]_1)=1]-\Pr[\mathcal{A}(\mathbb{G},D,[\mathbf{t}_1]_1)=1]|$$

where

$$D := (\,[\mathbf{B}_1]_2,[\mathbf{B}_2]_2,[\mathbf{B}_3]_2,[\mathbf{B}_4]_2,\mathsf{basis}(\mathbf{B}_2^\parallel),\mathsf{basis}(\mathbf{B}_1^\parallel,\mathbf{B}_3^\parallel,\mathbf{B}_4^\parallel)\,),$$
$$\mathbf{t}_0 \leftarrow \mathsf{span}(\mathbf{B}_1,\mathbf{B}_4),\ \mathbf{t}_1 \leftarrow \mathsf{span}(\mathbf{B}_1,\mathbf{B}_3,\mathbf{B}_4).$$

The proof is analogous to that for Lemma 1 (cf. [13]).

Also, we replace $\mathrm{SD}^{G_2}_{\mathbf{B}_3\mapsto\mathbf{B}_3,\mathbf{B}_2}$ assumption in Section 3.3 with *external subspace decision assumption* $\mathrm{XSD}^{G_2}_{\mathbf{B}_3,\mathbf{B}_4\mapsto\mathbf{B}_2,\mathbf{B}_3,\mathbf{B}_4}$ defined as below.

Assumption 3 ($\mathrm{XSD}^{G_2}_{\mathbf{B}_3,\mathbf{B}_4\mapsto\mathbf{B}_2,\mathbf{B}_3,\mathbf{B}_4}$) *We say that $\mathrm{XSD}^{G_2}_{\mathbf{B}_3,\mathbf{B}_4\mapsto\mathbf{B}_2,\mathbf{B}_3,\mathbf{B}_4}$ assumption holds if there exists an efficient sampler outputting random* $([\mathbf{B}_1]_2,[\mathbf{B}_2]_2,[\mathbf{B}_3]_2,[\mathbf{B}_4]_2)$ *along with base* $\mathsf{basis}(\mathbf{B}_1^\parallel),\mathsf{basis}(\mathbf{B}_4^\parallel)$ *and* $[\mathsf{basis}(\mathbf{B}_2^\parallel,\mathbf{B}_3^\parallel)]_1$ *(of arbitrary choice) such that the following advantage function is negligible in λ.*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{XSD}^{G_2}_{\mathbf{B}_3,\mathbf{B}_4\mapsto\mathbf{B}_2,\mathbf{B}_3,\mathbf{B}_4}}(\lambda) := |\Pr[\mathcal{A}(\mathbb{G},D,[\mathbf{t}_0]_1)=1]-\Pr[\mathcal{A}(\mathbb{G},D,[\mathbf{t}_1]_1)=1]|$$

where

$$D := (\,[\mathbf{B}_1]_2,[\mathbf{B}_2]_2,[\mathbf{B}_3]_2,[\mathbf{B}_4]_2,\mathsf{basis}(\mathbf{B}_1^\parallel),[\mathsf{basis}(\mathbf{B}_2^\parallel,\mathbf{B}_3^\parallel)]_1,\mathsf{basis}(\mathbf{B}_4^\parallel)\,),$$
$$\mathbf{t}_0 \leftarrow \mathsf{span}(\mathbf{B}_3,\mathbf{B}_4),\ \mathbf{t}_1 \leftarrow \mathsf{span}(\mathbf{B}_2,\mathbf{B}_3,\mathbf{B}_4).$$

We note that we do not give out $\mathsf{basis}(\mathbf{B}_2^\parallel,\mathbf{B}_3^\parallel,\mathbf{B}_4^\parallel)$ as usual; instead, $\mathsf{basis}(\mathbf{B}_4^\parallel)$ on $\mathbb{Z}_p$ and $[\mathsf{basis}(\mathbf{B}_2^\parallel,\mathbf{B}_3^\parallel)]_1$ on G_1 are provided. We then prove the following lemma saying that, for a specific set of parameters, the assumption is implied by XDLIN assumption.

Lemma 15 ($\text{XDLIN} \Rightarrow \text{XSD}^{G_2}_{\mathbf{B}_3,\mathbf{B}_4\mapsto\mathbf{B}_2,\mathbf{B}_3,\mathbf{B}_4}$). *Under the external decisional linear assumption* (XDLIN) *[1] (cf. Section 2.2), the* $\text{XSD}^{G_2}_{\mathbf{B}_3,\mathbf{B}_4\mapsto\mathbf{B}_2,\mathbf{B}_3,\mathbf{B}_4}$ *assumption holds for parameter* $\ell_2 = \ell_3 = \ell_4 = 1$.

Proof. For any PPT adversary $\mathcal{A}$, we construct an algorithm $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that

$$\mathsf{Adv}_{\mathcal{A}}^{\text{XSD}^{G_2}_{\mathbf{B}_3,\mathbf{B}_4\mapsto\mathbf{B}_2,\mathbf{B}_3,\mathbf{B}_4}}(\lambda) \le \mathsf{Adv}_{\mathcal{B}}^{\text{XDLIN}}(\lambda).$$

On input $([a_1,a_2,a_3,a_1s_1,a_2s_2]_1,[a_1,a_2,a_3,a_1s_1,a_2s_2]_2,T)$ where $a_1,a_2,a_3,s_1,s_2 \leftarrow \mathbb{Z}_p$ and T is either $[a_3(s_1+s_2)]_2$ or uniformly distributed over G_2, algorithm $\mathcal{B}$ works as follows:

Programming $\mathbf{B}_1,\mathbf{B}_2,\mathbf{B}_3,\mathbf{B}_4$ and $\mathbf{B}_1^{\|},\mathbf{B}_2^{\|},\mathbf{B}_3^{\|},\mathbf{B}_4^{\|}$. Sample $\widetilde{\mathbf{B}} \leftarrow \mathrm{GL}_{3+\ell_1}(\mathbb{Z}_p)$ and define

$$(\mathbf{B}_1,\mathbf{B}_2,\mathbf{B}_3,\mathbf{B}_4) = \widetilde{\mathbf{B}}\begin{pmatrix} \mathbf{I}_{\ell_1} & & & \\ & 1 & a_3 & a_3 \\ & & a_2 & \\ & & & a_1 \end{pmatrix} \quad\text{and}\quad (\mathbf{B}_1^{\|},\mathbf{B}_2^{\|},\mathbf{B}_3^{\|},\mathbf{B}_4^{\|}) = \widetilde{\mathbf{B}}^*\begin{pmatrix} \mathbf{I}_{\ell_1} & & & \\ & 1 & & \\ & -a_3a_2^{-1} & a_2^{-1} & \\ & -a_3a_1^{-1} & & a_1^{-1} \end{pmatrix}$$

Algorithm $\mathcal{B}$ can simulate $[\mathbf{B}_1,\mathbf{B}_2,\mathbf{B}_3,\mathbf{B}_4]_2$ using $[a_1,a_2,a_3]_2$.

Simulating $\mathsf{basis}(\mathbf{B}_1^{\|}),\mathsf{basis}(\mathbf{B}_4^{\|})$. We define

$$\mathsf{basis}(\mathbf{B}_1^{\|}) = \widetilde{\mathbf{B}}^*\begin{pmatrix} \mathbf{I}_{\ell_1} \\ \mathbf{0} \end{pmatrix} \quad\text{and}\quad \mathsf{basis}(\mathbf{B}_4^{\|}) = \widetilde{\mathbf{B}}^*(a_1^{-1}\mathbf{e}_{3+\ell_1})a_1 = \widetilde{\mathbf{B}}^*\mathbf{e}_{3+\ell_1},$$

both of which can be simulated using $\widetilde{\mathbf{B}}^*$.

Simulating $[\mathsf{basis}(\mathbf{B}_2^{\|},\mathbf{B}_3^{\|})]_1$. We define

$$\mathsf{basis}(\mathbf{B}_2^{\|},\mathbf{B}_3^{\|}) = \widetilde{\mathbf{B}}^*\begin{pmatrix} \mathbf{0} & \\ 1 & \\ -a_3a_2^{-1} & a_2^{-1} \\ -a_3a_1^{-1} & \end{pmatrix}\begin{pmatrix} a_1 & \\ a_1a_3 & a_2 \end{pmatrix} = \widetilde{\mathbf{B}}^*\begin{pmatrix} \mathbf{0} & \\ a_1 & \\ & 1 \\ -a_3 & \end{pmatrix}$$

such that $[\mathsf{basis}(\mathbf{B}_2^{\|},\mathbf{B}_3^{\|})]_1$ (over G_1) can be simulated using $\widetilde{\mathbf{B}}^*$ and $[a_1,a_3]_1$.

Simulating the challenge. Output the challenge

$$\begin{pmatrix} [\mathbf{0}]_2 \\ T \\ [a_2s_2]_2 \\ [a_1s_1]_2 \end{pmatrix}.$$

Observe that if $T = [a_3(s_1+s_2)]_2$, the output challenge is uniformly distributed over $[\mathsf{span}(\mathbf{B}_3,\mathbf{B}_4)]_2$; otherwise, if T is uniformly distributed over G_2, the output challenge is then uniformly distributed over $[\mathsf{span}(\mathbf{B}_2,\mathbf{B}_3,\mathbf{B}_4)]_2$. This readily proves the lemma. $\square$

4.2 Step One: A Private-key IPE from XDLIN Assumption

Our second private-key IPE is described as follows, which is translated from the private-key IPE in Section 3.2 with the correspondence (10). Here we employ the basis defined in Section 4.1 with parameter $(\ell_1,\ell_2,\ell_3,\ell_4) = (1,1,1,1)$.

- $\mathsf{Setup}(1^\lambda, n)$: Run $\mathbb{G} = (p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}(1^\lambda)$. Sample $\mathbf{B}_{14} = (\mathbf{B}_1|\mathbf{B}_4) \leftarrow \mathbb{Z}_p^{4\times 2}$ and pick $\mathbf{u}, \mathbf{w}_1, \ldots, \mathbf{w}_n \leftarrow \mathbb{Z}_p^{1\times 4}$, $\alpha \leftarrow \mathbb{Z}_p$. Output
$$\mathsf{msk} = (\mathbb{G}, \alpha, \mathbf{u}, \mathbf{w}_1, \ldots, \mathbf{w}_n, \mathbf{B}_{14}).$$
- $\mathsf{KeyGen}(\mathsf{msk}, \mathbf{y})$: Let $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{Z}_p^n$. Sample $\mathbf{r} \leftarrow \mathbb{Z}_p^2$ and output
$$\mathsf{sk}_{\mathbf{y}} = (K_0 = [\alpha + (y_1 \cdot \mathbf{w}_1 + \cdots + y_n \cdot \mathbf{w}_n)\mathbf{B}_{14}\mathbf{r}]_2, K_1 = [\mathbf{B}_{14}\mathbf{r}]_2)$$
- $\mathsf{Enc}(\mathsf{msk}, \mathbf{x}, m)$: Let $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}_p^n$ and $m \in G_T$. Output
$$\mathsf{ct}_{\mathbf{x}} = (C_1 = [x_1 \cdot \mathbf{u} + \mathbf{w}_1]_1, \ldots, C_n = [x_n \cdot \mathbf{u} + \mathbf{w}_n]_1, C = [\alpha]_T \cdot m)$$
- $\mathsf{Dec}(\mathsf{ct}_{\mathbf{x}}, \mathsf{sk}_{\mathbf{y}})$: Parse $\mathsf{ct}_{\mathbf{x}} = (C_1, \ldots, C_n, C)$ and $\mathsf{sk}_{\mathbf{y}} = (K_0, K_1)$ for $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{Z}_p^n$. Output
$$m' = C \cdot e(y_1 \odot C_1 \cdots y_n \odot C_n, K_1) \cdot e([1]_1, K_0)^{-1}.$$

Compared with the construction in Section 3.2, we now have ciphertexts over G_1 instead of $\mathbb{Z}_p$ and the bilinear map is required for decryption procedure. However the total dimension $\ell = 4$ is smaller than that in Section 3.1 when $k = 2$ (corresponding to DLIN assumption), which is $\ell = 5$.

Correctness. For all $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_p^n$ satisfying $\langle \mathbf{x}, \mathbf{y} \rangle = 0$, we have

$$\begin{aligned}
&e(y_1 \odot C_1 \cdots y_n \odot C_n, K_1) \cdot e([1]_1, K_0)^{-1} \\
=\;& e([y_1 \cdot (x_1 \cdot \mathbf{u} + \mathbf{w}_1) + \cdots + y_n \cdot (x_n \cdot \mathbf{u} + \mathbf{w}_n)]_1, [\mathbf{B}_{14}\mathbf{r}]_2) \cdot [\alpha + (y_1 \cdot \mathbf{w}_1 + \cdots + y_n \cdot \mathbf{w}_n)\mathbf{B}_{14}\mathbf{r}]_T^{-1} \\
=\;& [\langle \mathbf{x}, \mathbf{y} \rangle \cdot \mathbf{u}\mathbf{B}_{14}\mathbf{r}]_T \cdot [(y_1 \cdot \mathbf{w}_1 + \cdots + y_n \cdot \mathbf{w}_n)\mathbf{B}_{14}\mathbf{r}]_T \cdot [\alpha]_T^{-1} \cdot [(y_1 \cdot \mathbf{w}_1 + \cdots + y_n \cdot \mathbf{w}_n)\mathbf{B}_{14}\mathbf{r}]_T^{-1} = [\alpha]_T^{-1}
\end{aligned}$$

where the last equality follows from the fact that $\langle \mathbf{x}, \mathbf{y} \rangle = 0$. This readily proves the correctness.

4.3 Security

We will prove the following theorem.

Theorem 3. *Under the* XDLIN *assumption, the private-key IPE scheme described in Section 4.2 is adaptively secure and fully attribute-hiding (cf. Section 2.1).*

As before, we only need to prove the following lemma for $m_0 = m_1$.

Lemma 16. *For any adversary $\mathcal{A}$ that makes at most Q key queries and outputs $m_0 = m_1$, there exists adversaries $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$ such that*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{IPE}^*}(\lambda) \leq Q \cdot \mathsf{Adv}_{\mathcal{B}_1}^{\mathrm{SD}^{G_2}_{\mathbf{B}_1,\mathbf{B}_4 \mapsto \mathbf{B}_1,\mathbf{B}_3,\mathbf{B}_4}}(\lambda) + Q \cdot \mathsf{Adv}_{\mathcal{B}_2}^{\mathrm{XSD}^{G_2}_{\mathbf{B}_3,\mathbf{B}_4 \mapsto \mathbf{B}_2,\mathbf{B}_3,\mathbf{B}_4}}(\lambda) + Q \cdot \mathsf{Adv}_{\mathcal{B}_3}^{\mathrm{SD}^{G_2}_{\mathbf{B}_1,\mathbf{B}_4 \mapsto \mathbf{B}_1,\mathbf{B}_3,\mathbf{B}_4}}(\lambda)$$

and $\mathsf{Time}(\mathcal{B}_1), \mathsf{Time}(\mathcal{B}_2), \mathsf{Time}(\mathcal{B}_3) \approx \mathsf{Time}(\mathcal{A})$.

Game sequence. With the correspondence in Section 4.1, the proof for lemma 16 is almost the same as that for Lemma 2 presented in Section 3. Here we only give the game sequence, summarized in Fig 4.

- Game_0 is the real game in which the challenge ciphertext for $\mathbf{x}_b = (x_{1,b}, \ldots, x_{n,b})$ is of the form
$$[x_{1,b} \cdot \mathbf{u} + \mathbf{w}_1]_1, \ldots, [x_{n,b} \cdot \mathbf{u} + \mathbf{w}_n]_1, [\alpha]_T \cdot m_0.$$
Here $b \leftarrow \{0,1\}$ is a secret bit.
- Game_1 is identical to Game_0 except that the challenge ciphertext is
$$[x_{1,b} \cdot \mathbf{u}^{(134)} + \boxed{x_{1,1-b} \cdot \mathbf{u}^{(2)}} + \mathbf{w}_1]_1, \ldots, [x_{n,b} \cdot \mathbf{u}^{(134)} + \boxed{x_{n,1-b} \cdot \mathbf{u}^{(2)}} + \mathbf{w}_n]_1, [\alpha]_T \cdot m_0.$$
We claim that $\mathsf{Game}_1 \equiv \mathsf{Game}_0$. The proof is analogous to that for $\mathsf{Game}_1 \equiv \mathsf{Game}_0$ in Section 3.3.

Game	ct			κ-th sk ($\mathbf{d} \leftarrow \mathsf{span}(?)$)			Remark
	$?^{(14)} + \mathbf{w}_i^{(14)}$	$?^{(2)} + \mathbf{w}_i^{(2)}$	$?^{(3)} + \mathbf{w}_i^{(3)}$	$\kappa < j$	$\kappa = j$	$\kappa > j$	
0	$x_{i,b} \cdot \mathbf{u}$			$\mathbf{B}_1, \mathbf{B}_4$			real game
1	$x_{i,b} \cdot \mathbf{u}$	$x_{i,1-b} \cdot \mathbf{u}$	$x_{i,b} \cdot \mathbf{u}$	$\mathbf{B}_1, \mathbf{B}_4$			statistical argument: analogous to Fig 3
$2.j-1$	$x_{i,b} \cdot \mathbf{u}$	$x_{i,1-b} \cdot \mathbf{u}$	$x_{i,b} \cdot \mathbf{u}$	$\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_4$	$\mathbf{B}_1, \mathbf{B}_4$	$\mathbf{B}_1, \mathbf{B}_4$	$\mathsf{Game}_{2.0} = \mathsf{Game}_1$, $\mathsf{Game}_{2.j} = \mathsf{Game}_{2.j-1.5}$
$2.j-1.1$	$x_{i,b} \cdot \mathbf{u}$	$x_{i,1-b} \cdot \mathbf{u}$	$x_{i,b} \cdot \mathbf{u}$	$\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_4$	$\mathbf{B}_1, \mathbf{B}_3, \mathbf{B}_4$	$\mathbf{B}_1, \mathbf{B}_4$	$\mathrm{SD}^{G_2}_{\mathbf{B}_1,\mathbf{B}_4 \mapsto \mathbf{B}_1,\mathbf{B}_3,\mathbf{B}_4}$: given $\mathsf{basis}(\mathbf{B}_2^{\Vert})$, $\mathsf{basis}(\mathbf{B}_1^{\Vert}, \mathbf{B}_3^{\Vert}, \mathbf{B}_4^{\Vert})$, $[\mathsf{span}(\mathbf{B}_1, \mathbf{B}_4)]_2 \approx_c [\mathsf{span}(\mathbf{B}_1, \mathbf{B}_3, \mathbf{B}_4)]_2$
$2.j-1.2$	$x_{i,b} \cdot \mathbf{u}$	$x_{i,1-b} \cdot \mathbf{u}$	$x_{i,1-b} \cdot \mathbf{u}$	$\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_4$	$\mathbf{B}_1, \mathbf{B}_3, \mathbf{B}_4$	$\mathbf{B}_1, \mathbf{B}_4$	statistical argument: analogous to Fig 3
$2.j-1.3$	$x_{i,b} \cdot \mathbf{u}$	$x_{i,1-b} \cdot \mathbf{u}$	$x_{i,1-b} \cdot \mathbf{u}$	$\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_4$	$\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3, \mathbf{B}_4$	$\mathbf{B}_1, \mathbf{B}_4$	$\mathrm{XSD}^{G_2}_{\mathbf{B}_3,\mathbf{B}_4 \mapsto \mathbf{B}_2,\mathbf{B}_3,\mathbf{B}_4}$: given $[\mathsf{basis}(\mathbf{B}_2^{\Vert}, \mathbf{B}_3^{\Vert})]_1$, $\mathsf{basis}(\mathbf{B}_1^{\Vert})$, $\mathsf{basis}(\mathbf{B}_4^{\Vert})$, $[\mathsf{span}(\mathbf{B}_3, \mathbf{B}_4)]_2 \approx_c [\mathsf{span}(\mathbf{B}_2, \mathbf{B}_3, \mathbf{B}_4)]_2$
$2.j-1.4$	$x_{i,b} \cdot \mathbf{u}$	$x_{i,1-b} \cdot \mathbf{u}$	$x_{i,b} \cdot \mathbf{u}$	$\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_4$	$\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3, \mathbf{B}_4$	$\mathbf{B}_1, \mathbf{B}_4$	statistical argument: analogous to $\mathsf{Game}_{2.j-1.2}$
$2.j-1.5$	$x_{i,b} \cdot \mathbf{u}$	$x_{i,1-b} \cdot \mathbf{u}$	$x_{i,b} \cdot \mathbf{u}$	$\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_4$	$\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_4$	$\mathbf{B}_1, \mathbf{B}_4$	$\mathrm{SD}^{G_2}_{\mathbf{B}_1,\mathbf{B}_4 \mapsto \mathbf{B}_1,\mathbf{B}_3,\mathbf{B}_4}$: analogous to $\mathsf{Game}_{2.j-1.1}$
3	$x_{i,0} \cdot \mathbf{u}_0 + x_{i,1} \cdot \mathbf{u}_1$		$x_{i,b} \cdot \mathbf{u}$	$\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_4$			$\mathbf{u}_0, \mathbf{u}_1 \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$; change of basis
4	$x_{i,0} \cdot \mathbf{u}_0 + x_{i,1} \cdot \mathbf{u}_1$			$\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_4$			statistical argument: analogous to Game_1

Fig. 4. Game sequence for Private-key IPE based on XDLIN. The gray background highlights the difference between adjacent games.

- $\mathsf{Game}_{2.j}$ for $j \in [0, q]$ is identical to Game_1 except that the first j secret keys are

$$[\alpha + (y_1 \cdot \mathbf{w}_1 + \cdots + y_n \cdot \mathbf{w}_n)\mathbf{d}]_2,\ [\mathbf{d}]_2 \quad \text{where} \quad \boxed{\mathbf{d} \leftarrow \mathsf{span}(\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_4)}.$$

  We claim that $\mathsf{Game}_{2.j-1} \approx_c \mathsf{Game}_{2.j}$ for $j \in [q]$ and give a proof sketch later.
- Game_3 is identical to $\mathsf{Game}_{2.q}$ except that the challenge ciphertext is

$$[\boxed{x_{1,0} \cdot \mathbf{u}_0^{(124)} + x_{1,1} \cdot \mathbf{u}_1^{(124)}} + x_{1,b} \cdot \mathbf{u}^{(3)} + \mathbf{w}_1]_1, \ldots, [\boxed{x_{n,0} \cdot \mathbf{u}_0^{(124)} + x_{n,1} \cdot \mathbf{u}_1^{(124)}} + x_{n,b} \cdot \mathbf{u}^{(3)} + \mathbf{w}_n]_1,\ [\alpha]_T \cdot m_0.$$

  where $\mathbf{u}_0, \mathbf{u}_1 \leftarrow \mathbb{Z}_p^{1\times(k+1)}$. We claim that $\mathsf{Game}_{2.q} \equiv \mathsf{Game}_3$. The proof is analogous to that for $\mathsf{Game}_{2.q} \equiv \mathsf{Game}_3$ in Section 3.3 using "change of basis" technique [23, 28], except that we now work with subspace $\mathsf{span}(\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_4)$ corresponding to $\mathsf{span}(\mathbf{B}_1, \mathbf{B}_2)$ there (cf. Section 4.1).
- Game_4 is identical to Game_3 except that the challenge ciphertext is

$$[\boxed{x_{1,0} \cdot \mathbf{u}_0 + x_{1,1} \cdot \mathbf{u}_1} + \mathbf{w}_1]_1, \ldots, [\boxed{x_{n,0} \cdot \mathbf{u}_0 + x_{n,1} \cdot \mathbf{u}_1} + \mathbf{w}_n]_1,\ [\alpha]_T \cdot m_0$$

  We claim that $\mathsf{Game}_3 \equiv \mathsf{Game}_4$ and the adversary has no advantage in guessing b in Game_4. The proof for the former claim is similar to that for $\mathsf{Game}_1 \equiv \mathsf{Game}_0$.

Proving $\mathsf{Game}_{2.j-1} \approx_c \mathsf{Game}_{2.j}$. We now proves $\mathsf{Game}_{2.j-1} \approx_c \mathsf{Game}_{2.j}$ which completes the proof for Lemma 16. For all $j \in [q]$, we employ the following game sequence, which has been included in Fig 4.

- $\mathsf{Game}_{2.j-1.1}$ is identical to $\mathsf{Game}_{2.j-1}$ except that the jth secret key is

$$[\alpha + (y_1 \cdot \mathbf{w}_1 + \cdots + y_n \cdot \mathbf{w}_n)\mathbf{d}]_2,\ [\mathbf{d}]_2 \quad \text{where} \quad \boxed{\mathbf{d} \leftarrow \mathsf{span}(\mathbf{B}_1, \mathbf{B}_3, \mathbf{B}_4)}.$$

  We claim that $\mathsf{Game}_{2.j-1.1} \approx_c \mathsf{Game}_{2.j-1}$. This follows from the $\mathrm{SD}^{G_2}_{\mathbf{B}_1,\mathbf{B}_4 \mapsto \mathbf{B}_1,\mathbf{B}_3,\mathbf{B}_4}$ assumption with a reduction analogous to that for $\mathsf{Game}_{2.j-1.1} \approx_c \mathsf{Game}_{2.j-1}$ in Section 3.3.
- $\mathsf{Game}_{2.j-1.2}$ is identical to $\mathsf{Game}_{2.j-1.1}$ except that the challenge ciphertext is

$$[x_{1,b} \cdot \mathbf{u}^{(14)} + x_{1,1-b} \cdot \mathbf{u}^{(2)} + \boxed{x_{1,1-b} \cdot \mathbf{u}^{(3)}} + \mathbf{w}_1]_1, \ldots, [x_{n,b} \cdot \mathbf{u}^{(14)} + x_{n,1-b} \cdot \mathbf{u}^{(2)} + \boxed{x_{n,1-b} \cdot \mathbf{u}^{(3)}} + \mathbf{w}_n]_1, [\alpha]_T \cdot m_0.$$

We claim that $\mathsf{Game}_{2.j-1.2} \equiv \mathsf{Game}_{2.j-1.1}$. The proof is analogous to that for $\mathsf{Game}_{2.j-1.2} \equiv \mathsf{Game}_{2.j-1.1}$ in Section 3.3.

- $\mathsf{Game}_{2.j-1.3}$ is identical to $\mathsf{Game}_{2.j-1.2}$ except that the j-th secret key is

$$[\alpha + (y_1 \cdot \mathbf{w}_1 + \cdots + y_n \cdot \mathbf{w}_n)\mathbf{d}]_2,\ [\mathbf{d}]_2 \quad \text{where} \quad \boxed{\mathbf{d} \leftarrow \mathsf{span}(\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3, \mathbf{B}_4)}.$$

  We claim that $\mathsf{Game}_{2.j-1.3} \approx_c \mathsf{Game}_{2.j-1.2}$. This follows from the $\text{XSD}^{G_2}_{\mathbf{B}_3,\mathbf{B}_4 \mapsto \mathbf{B}_2,\mathbf{B}_3,\mathbf{B}_4}$ assumption. The proof is analogous to that for $\mathsf{Game}_{2.j-1.3} \equiv \mathsf{Game}_{2.j-1.2}$ in Section 3.3. Note that, in the reduction, we simulate the challenge ciphertext over G_1 using $[\mathsf{basis}(\mathbf{B}_2^{\|}, \mathbf{B}_3^{\|})]_1$.
- $\mathsf{Game}_{2.j-1.4}$ is identical to $\mathsf{Game}_{2.j-1.3}$ except that the challenge ciphertext is

$$[x_{1,b} \cdot \mathbf{u}^{(14)} + x_{1,1-b} \cdot \mathbf{u}^{(2)} + \boxed{x_{1,b} \cdot \mathbf{u}^{(3)}} + \mathbf{w}_1]_1, \ldots, [x_{n,b} \cdot \mathbf{u}^{(14)} + x_{n,1-b} \cdot \mathbf{u}^{(2)} + \boxed{x_{n,b} \cdot \mathbf{u}^{(3)}} + \mathbf{w}_n]_1, [\alpha]_T \cdot m_0.$$

  We claim that $\mathsf{Game}_{2.j-1.4} \equiv \mathsf{Game}_{2.j-1.3}$. The proof is identical to that for $\mathsf{Game}_{2.j-1.2} \equiv \mathsf{Game}_{2.j-1.1}$.
- $\mathsf{Game}_{2.j-1.5}$ is identical to $\mathsf{Game}_{2.j-1.4}$ except that the jth secret key is

$$[\alpha + (y_1 \cdot \mathbf{w}_1 + \cdots + y_n \cdot \mathbf{w}_n)\mathbf{d}]_2,\ [\mathbf{d}]_2 \quad \text{where} \quad \boxed{\mathbf{d} \leftarrow \mathsf{span}(\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_4)}.$$

  We claim that $\mathsf{Game}_{2.j-1.5} \approx_c \mathsf{Game}_{2.j-1.4}$. The proof is identical to that for $\mathsf{Game}_{2.j-1} \approx_c \mathsf{Game}_{2.j-1.1}$. Note that $\mathsf{Game}_{2.j-1.5} = \mathsf{Game}_{2.j}$.

4.4 Step Two: From private-key to public-key

Following the "private-key to public-key" compiler [36], we transform the private-key IPE in Section 4.2 to the following public-key IPE:

- $\mathsf{Setup}(1^\lambda, n)$: Run $\mathbb{G} = (p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}(1^\lambda)$. Sample $\mathbf{A} \leftarrow \mathbb{Z}_p^{3\times 2}, \mathbf{B}_{14} \leftarrow \mathbb{Z}_p^{4\times 2}$ and pick

$$\mathbf{U}, \mathbf{W}_1, \ldots, \mathbf{W}_n \leftarrow \mathbb{Z}_p^{3\times 4} \quad \text{and} \quad \mathbf{k} \leftarrow \mathbb{Z}_p^3.$$

  Output

$$\mathsf{mpk} = (\mathbb{G}, [\mathbf{A}^\top]_1, [\mathbf{A}^\top \mathbf{U}]_1, [\mathbf{A}^\top \mathbf{W}_1]_1, \ldots, [\mathbf{A}^\top \mathbf{W}_n]_1, [\mathbf{A}^\top \mathbf{k}]_T) \quad \text{and} \quad \mathsf{msk} = (\mathbf{k}, \mathbf{W}_1, \ldots, \mathbf{W}_n, \mathbf{B}_{14}).$$

- $\mathsf{KeyGen}(\mathsf{msk}, \mathbf{y})$: Let $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{Z}_p^n$. Sample $\mathbf{r} \leftarrow \mathbb{Z}_p^2$ and output

$$\mathsf{sk}_{\mathbf{y}} = (K_0 = [\mathbf{k} + (y_1 \cdot \mathbf{W}_1 + \cdots + y_n \cdot \mathbf{W}_n)\mathbf{B}_{14}\mathbf{r}]_2, K_1 = [\mathbf{B}_{14}\mathbf{r}]_2)$$

- $\mathsf{Enc}(\mathsf{mpk}, \mathbf{x}, m)$: Let $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}_p^n$ and $m \in G_T$. Sample $\mathbf{s} \leftarrow \mathbb{Z}_p^2$ and output

$$\mathsf{ct}_{\mathbf{x}} = (C_0 = [\mathbf{s}^\top \mathbf{A}^\top]_1, C_1 = [\mathbf{s}^\top \mathbf{A}^\top (x_1 \cdot \mathbf{U} + \mathbf{W}_1)]_1, \ldots, C_n = [\mathbf{s}^\top \mathbf{A}^\top (x_n \cdot \mathbf{U} + \mathbf{W}_n)]_1, C = [\mathbf{s}^\top \mathbf{A}^\top \mathbf{k}]_T \cdot m)$$

- $\mathsf{Dec}(\mathsf{ct}_{\mathbf{x}}, \mathsf{sk}_{\mathbf{y}})$: Parse $\mathsf{ct}_{\mathbf{x}} = (C_0, C_1, \ldots, C_n, C)$ and $\mathsf{sk}_{\mathbf{y}} = (K_0, K_1)$ for $\mathbf{y} = (y_1, \ldots, y_n)$. Output

$$m' = C \cdot e(y_1 \odot C_1 \cdots y_n \odot C_n, K_1) \cdot e(C_0, K_0)^{-1}.$$

The correctness can be verified as in Section 3.4.

Security. We will prove the following theorem.

Theorem 4. *Under the* XDLIN *assumption, the IPE scheme described above is adaptively secure and fully attribute-hiding (cf. Section 2.1).*

Concretely, we prove the following lemma, showing that the security of the above IPE is implied by that of our private-key IPE in Section 4.2 and the MDDH_2 assumption.

Lemma 17. *For any adversary $\mathcal{A}$ that makes at most Q key queries, there exists adversaries $\mathcal{B}_0, \mathcal{B}$ such that*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{IPE}}(\lambda) \leq \mathsf{Adv}_{\mathcal{B}_0}^{\mathrm{MDDH}_2}(\lambda) + \mathsf{Adv}_{\mathcal{B}}^{\mathrm{IPE}^*}(\lambda)$$

and $\mathsf{Time}(\mathcal{B}_0), \mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$.

We prove Lemma 17 via the following game sequence, as in Section 3.4.

- Game_0 is the real game in which the challenge ciphertext for $\mathbf{x}_b = (x_{1,b}, \ldots, x_{n,b})$ is of the form

$$[\mathbf{c}^\top]_1, [\mathbf{c}^\top(x_{1,b} \cdot \mathbf{U} + \mathbf{W}_1)]_1, \ldots, [\mathbf{c}^\top(x_{n,b} \cdot \mathbf{U} + \mathbf{W}_n)]_1, e([\mathbf{c}^\top]_1, [\mathbf{k}]_2) \cdot m_b \quad \text{where} \quad \mathbf{c} \leftarrow \mathsf{span}(\mathbf{A}).$$

  Here $b \leftarrow \{0,1\}$ is a secret bit.
- Game_1 is identical to Game_0 except that we sample $\mathbf{c} \leftarrow \mathbb{Z}_p^{k+1}$ when generating the challenge ciphertext. We claim that $\mathsf{Game}_1 \approx_c \mathsf{Game}_0$. This follows from MDDH_2 assumption and the proof is analogous to that for $\mathsf{Game}_1 \approx_c \mathsf{Game}_0$ in Section 3.4.

Analogous to Section 3.4 and Section 3.6, we can prove that adversary's advantage in Game_1 is bounded by that against our private-key IPE in Section 4.2.

Acknowledgement. We thank the reviewers for their detailed and constructive feedback.

References

[1] M. Abe, M. Chase, B. David, M. Kohlweiss, R. Nishimaki, and M. Ohkubo. Constant-size structure-preserving signatures: Generic constructions and simple assumptions. In X. Wang and K. Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 4–24. Springer, Heidelberg, Dec. 2012.

[2] S. Agrawal and M. Chase. A study of pair encodings: Predicate encryption in prime order groups. In E. Kushilevitz and T. Malkin, editors, *TCC 2016-A, Part II*, volume 9563 of *LNCS*, pages 259–288. Springer, Heidelberg, Jan. 2016.

[3] S. Agrawal and M. Chase. Simplifying design and analysis of complex predicate encryption schemes. In J. Coron and J. B. Nielsen, editors, *EUROCRYPT 2017, Part I*, volume 10210 of *LNCS*, pages 627–656. Springer, Heidelberg, May 2017.

[4] N. Attrapadung. Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more. In P. Q. Nguyen and E. Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 557–577. Springer, Heidelberg, May 2014.

[5] N. Attrapadung. Dual system encryption framework in prime-order groups via computational pair encodings. In J. H. Cheon and T. Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 591–623. Springer, Heidelberg, Dec. 2016.

[6] N. Attrapadung and S. Yamada. Duality in ABE: Converting attribute based encryption for dual predicate and dual policy via computational encodings. In K. Nyberg, editor, *CT-RSA 2015*, volume 9048 of *LNCS*, pages 87–105. Springer, Heidelberg, Apr. 2015.

[7] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *2007 IEEE Symposium on Security and Privacy*, pages 321–334. IEEE Computer Society Press, May 2007.

[8] D. Boneh and X. Boyen. Efficient selective-ID secure identity based encryption without random oracles. In C. Cachin and J. Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 223–238. Springer, Heidelberg, May 2004.

[9] D. Boneh, C. Gentry, S. Gorbunov, S. Halevi, V. Nikolaenko, G. Segev, V. Vaikuntanathan, and D. Vinayagamurthy. Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits. In P. Q. Nguyen and E. Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 533–556. Springer, Heidelberg, May 2014.

[10] D. Boneh and B. Waters. Conjunctive, subset, and range queries on encrypted data. In S. P. Vadhan, editor, *TCC 2007*, volume 4392 of *LNCS*, pages 535–554. Springer, Heidelberg, Feb. 2007.

[11] J. Chen, R. Gay, and H. Wee. Improved dual system ABE in prime-order groups via predicate encodings. In E. Oswald and M. Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 595–624. Springer, Heidelberg, Apr. 2015.

[12] J. Chen and J. Gong. ABE with tag made easy - concise framework and new instantiations in prime-order groups. In T. Takagi and T. Peyrin, editors, *ASIACRYPT 2017, Part II*, volume 10625 of *LNCS*, pages 35–65. Springer, Heidelberg, Dec. 2017.

[13] J. Chen, J. Gong, L. Kowalczyk, and H. Wee. Unbounded ABE via bilinear entropy expansion, revisited. In J. B. Nielsen and V. Rijmen, editors, *EUROCRYPT 2018, Part I*, volume 10820 of *LNCS*, pages 503–534, 2018.

[14] A. Escala, G. Herold, E. Kiltz, C. Ràfols, and J. Villar. An algebraic framework for Diffie-Hellman assumptions. In R. Canetti and J. A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 129–147. Springer, Heidelberg, Aug. 2013.

[15] R. Gay, D. Hofheinz, E. Kiltz, and H. Wee. Tightly CCA-secure encryption without pairings. In M. Fischlin and J.-S. Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 1–27. Springer, Heidelberg, May 2016.

[16] J. Gong, J. Chen, X. Dong, Z. Cao, and S. Tang. Extended nested dual system groups, revisited. In C.-M. Cheng, K.-M. Chung, G. Persiano, and B.-Y. Yang, editors, *PKC 2016, Part I*, volume 9614 of *LNCS*, pages 133–163. Springer, Heidelberg, Mar. 2016.

[17] J. Gong, X. Dong, J. Chen, and Z. Cao. Efficient IBE with tight reduction to standard assumption in the multi-challenge setting. In J. H. Cheon and T. Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 624–654. Springer, Heidelberg, Dec. 2016.

[18] S. Gorbunov, V. Vaikuntanathan, and H. Wee. Attribute-based encryption for circuits. In D. Boneh, T. Roughgarden, and J. Feigenbaum, editors, *45th ACM STOC*, pages 545–554. ACM Press, June 2013.

[19] S. Gorbunov, V. Vaikuntanathan, and H. Wee. Predicate encryption for circuits from LWE. In R. Gennaro and M. J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 503–523. Springer, Heidelberg, Aug. 2015.

[20] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In A. Juels, R. N. Wright, and S. Vimercati, editors, *ACM CCS 06*, pages 89–98. ACM Press, Oct. / Nov. 2006. Available as Cryptology ePrint Archive Report 2006/309.

[21] Y. Ishai and H. Wee. Partial garbling schemes and their applications. In J. Esparza, P. Fraigniaud, T. Husfeldt, and E. Koutsoupias, editors, *ICALP 2014, Part I*, volume 8572 of *LNCS*, pages 650–662. Springer, Heidelberg, July 2014.

[22] J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In N. P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 146–162. Springer, Heidelberg, Apr. 2008.

[23] A. B. Lewko. Tools for simulating features of composite order bilinear groups in the prime order setting. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 318–335. Springer, Heidelberg, Apr. 2012.

[24] 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 H. Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 62–91. Springer, Heidelberg, May 2010.

[25] A. B. Lewko and B. Waters. New proof methods for attribute-based encryption: Achieving full security through selective techniques. In R. Safavi-Naini and R. Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 180–198. Springer, Heidelberg, Aug. 2012.

[26] T. Okamoto and K. Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In T. Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 191–208. Springer, Heidelberg, Aug. 2010.

[27] T. Okamoto and K. Takashima. Adaptively attribute-hiding (hierarchical) inner product encryption. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 591–608. Springer, Heidelberg, Apr. 2012.

[28] T. Okamoto and K. Takashima. Fully secure unbounded inner-product and attribute-based encryption. In X. Wang and K. Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 349–366. Springer, Heidelberg, Dec. 2012.

[29] T. Okamoto and K. Takashima. Efficient (hierarchical) inner-product encryption tightly reduced from the decisional linear assumption. *IEICE Transactions*, 96-A(1):42–52, 2013.

[30] R. Ostrovsky, A. Sahai, and B. Waters. Attribute-based encryption with non-monotonic access structures. In P. Ning, S. D. C. di Vimercati, and P. F. Syverson, editors, *ACM CCS 07*, pages 195–203. ACM Press, Oct. 2007.

[31] A. Sahai and B. R. Waters. Fuzzy identity-based encryption. In R. Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 457–473. Springer, Heidelberg, May 2005.

[32] B. Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In S. Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 619–636. Springer, Heidelberg, Aug. 2009.

[33] B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, editors, *PKC 2011*, volume 6571 of *LNCS*, pages 53–70. Springer, Heidelberg, Mar. 2011.

[34] B. R. Waters. Efficient identity-based encryption without random oracles. In R. Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 114–127. Springer, Heidelberg, May 2005.

[35] H. Wee. Dual system encryption via predicate encodings. In Y. Lindell, editor, *TCC 2014*, volume 8349 of *LNCS*, pages 616–637. Springer, Heidelberg, Feb. 2014.

[36] H. Wee. Attribute-hiding predicate encryption in bilinear groups, revisited. In Y. Kalai and L. Reyzin, editors, *TCC 2017, Part I*, volume 10677 of *LNCS*, pages 206–233. Springer, Heidelberg, Nov. 2017.