Doubly Spatial Encryption from DBDH

Jie Chen[1,⋆] and Hoeteck Wee[2,⋆⋆]

[1] Department of Computer Science and Technology, East China Normal University
[2] École Normale Supérieure, Paris

Abstract. Functional encryption is an emerging paradigm for public-key encryption which enables fine-grained control of access to encrypted data. Doubly-spatial encryption (DSE) captures all functionalities that we know how to realize via pairings-based assumptions, including (H)IBE, IPE, NIPE, CP-ABE and KP-ABE. In this paper, we propose a construction of DSE from the decisional bilinear Diffie-Hellman (DBDH) assumption. This also yields the first non-zero inner product encryption (NIPE) scheme based on DBDH. Quite surprisingly, we know how to realize NIPE and DSE from stronger assumptions in bilinear groups but not from the basic DBDH assumption. Along the way, we present a novel algebraic characterization of NO instances for the DSE functionality, which we use crucially in the proof of security.

1 Introduction

Functional encryption is an emerging paradigm for public-key encryption which enables fine-grained control of access to encrypted data [18, 13]. In traditional public-key encryption, access to the encrypted data is all or nothing: given the secret key, one can decrypt and read the entire plaintext, but without it, nothing about the plaintext is revealed (other than its length). In functional encryption, ciphertext is associated with a value x and a secret key with a value y, and the secret key decrypts the ciphertext if and only if x and y satisfies some predicate. The security requirement is that of collusion resilience, namely any group of users collectively learns nothing about the plaintext if none of them is individually authorized to decrypt the ciphertext.

Much of the literature on functional encryption started with constructions based on the decisional bilinear Diffie-Hellman (DBDH) assumption [5]. Fix prime-order groups (G, G_T), endowed with an efficient symmetric bilinear map $e : G \times G \to G_T$. Let g denote a random generator of G. The DBDH assumption stipulates that given g, g^a, g^b, g^c, the quantity $e(g,g)^{abc}$ is pseudorandom. The DBDH assumption is extremely appealing in its simplicity: the assumption is simple to state, the ensuing schemes as well as the proof of security are typically extremely simple too; these schemes have also been standardized [8]. Furthermore, we continue to draw on the techniques developed in these early works: the development of lattice-based (hierarchical) identity-based encryption ((H)IBE) schemes in [11, 1, 2] parallel corresponding DBDH-based schemes in [10, 4, 20] and the simplest instantiations of the dual system encryption framework in [16, 17] proceed by "embedding" prior DBDH-based schemes into composite-order groups. The fundamental role that the DBDH assumption plays in functional encryption motivates us to understand the limitations on the functionalities that we can realize from the DBDH assumption: namely,

[⋆] Email: s080001@e.ntu.edu.sg. Supported by Science and Technology Commission of Shanghai Municipality under Grants 14YF1404200, 13JC1403500, and the National Natural Science Foundation of China Grant No. 61172085. Part of this work was done at Nanyang Technological University, supported by the National Research Foundation of Singapore under Research Grant NRF-CRP2-2007-03.

[⋆⋆] Email: wee@di.ens.fr. CNRS (UMR 8548) and INRIA. Supported in part by the French ANR-12-INSE-0014 SIMPATIC Project. Part of this work was done at George Washington University, supported by NSF Award CNS-1319021, and at Ruhr-Universität Bochum as a Research Fellow of the Alexander von Humboldt Foundation.

> Can we realize every functionality achievable via bilinear maps from the DBDH assumption?

State-of-the-art. The state-of-the-art for functional encryption from the DBDH assumption is roughly speaking, that of spatial encryption [6, 12], which generalizes (H)IBE, inner product encryption (IPE) and key-policy attribute-based encryption (KP-ABE) [4, 13, 15], as well as that of ciphertext-policy attribute-based encryption (CP-ABE) [19] (which is not captured by spatial encryption). In spatial encryption, a ciphertext is associated with a vector and a secret key with an affine space, and decryption is possible iff the affine space contains the vector. A further generalization of spatial encryption is that of doubly-spatial encryption (DSE) [14] where both the ciphertext and the secret key are associated with affine spaces, and decryption is possible iff the two affine spaces have non-empty intersection. Doubly-spatial encryption captures all functionalities that we know how to realize via pairings-based assumptions, including (H)IBE, IPE, non-zero inner product encryption (NIPE), CP-ABE and KP-ABE; in particular, we know how to capture NIPE and CP-ABE from doubly-spatial encryption but not from spatial encryption. Quite surprisingly, we know how to realize NIPE and DSE from stronger assumptions in bilinear groups [3, 14, 12][1] but not from the basic DBDH assumption.

1.1 Our Results

Our main result is a construction of doubly-spatial encryption (DSE) from the basic DBDH assumption. This also yields the first NIPE scheme based on DBDH, which in turn yields identity-based revocable crypto-systems [3]. Along the way, we present a novel algebraic characterization of NO instances for the DSE functionality (c.f. Lemma 1), which we use crucially in the proof of security. We compare our (D)SE schemes with prior works in Fig 1.

Reference		$\lvert\textsc{mpk}\rvert$	$\lvert\textsc{sk}\rvert$	$\lvert\textsc{ct}\rvert$	assumption
SE	BH [6]	$(n+2)\lvert G\rvert+\lvert G_T\rvert$	$(m+2)\lvert G\rvert$	$2\lvert G\rvert+\lvert G_T\rvert$	n-DBDHE
	ZC [20]	$(n+2)\lvert G\rvert+\lvert G_T\rvert$	$(n+m+1)\lvert G\rvert$	$(n+1)\lvert G\rvert+\lvert G_T\rvert$	DBDH
	Ours	$(2n^2+6n+5)\lvert G\rvert+\lvert G_T\rvert$	$(n+2)\lvert G\rvert$	$(n+2)\lvert G\rvert+\lvert G_T\rvert$	DBDH
DSE	Ham[14]	$(n+2)\lvert G\rvert+\lvert G_T\rvert$	$(m+2)\lvert G\rvert$	$(d+2)\lvert G\rvert+\lvert G_T\rvert$	n-DBDHE
	Ours	$(2n^2+6n+5)\lvert G\rvert+\lvert G_T\rvert$	$(n+2)\lvert G\rvert$	$(nd+n+d+2)\lvert G\rvert+\lvert G_T\rvert$	DBDH

Fig. 1. Comparison amongst selectively-secure DSE schemes, where the ciphertext is associated with $(\mathbf{x}_0, \mathbf{X}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^{n\times d}$ and the secret key is associated with $(\mathbf{y}_0, \mathbf{Y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^{n\times m}$ and decryption works whenever $(\mathbf{x}_0 + \text{span}(\mathbf{X})) \cap (\mathbf{y}_0 + \text{span}(\mathbf{Y})) \neq \emptyset$. Note that $d, m \leq n$. The parameters for our DSE scheme refers to that obtained by combining the construction in Section 3 and transformation in Appendix A. For SE, we set $d = 0$.

Warm-up. Before we present our construction, we define DSE more formally. In DSE, we associate a ciphertext with a vector matrix pair $(\mathbf{x}_0, \mathbf{X})$ specifying an affine space $\mathbf{x}_0 + \text{span}(\mathbf{X})$, and a secret

[1] In particular, the DSE and NIPE schemes in [12, 3] are based on the DLIN assumption, which implies the DBDH assumption [9].

Reference		$\lvert\mathrm{MPK}\rvert$	$\lvert\mathrm{SK}\rvert$	$\lvert\mathrm{CT}\rvert$	assumption	security
NIPE	AL[3]	$(2n+1)\lvert G\rvert+\lvert G_T\rvert$	$(n+1)\lvert G\rvert$	$3\lvert G\rvert+\lvert G_T\rvert$	q-MEBDH	co-selective
		$(n+11)\lvert G\rvert+\lvert G_T\rvert$	$(n+6)\lvert G\rvert$	$9\lvert G\rvert+\lvert G_T\rvert$	DBDH & DLIN	co-selective
	Ours	$(n^2+n+1)\lvert G\rvert+\lvert G_T\rvert$	$(n+1)\lvert G\rvert$	$(n+1)\lvert G\rvert+\lvert G_T\rvert$	DBDH	selective

Fig. 2. Comparison amongst existing and our (co-)selectively secure NIPE schemes, where the ciphertext is associated with $\mathbf{x}\in\mathbb{Z}_p^n$ and the secret key is associated with $\mathbf{y}\in\mathbb{Z}_p^n$ and decryption works whenever $\mathbf{x}\cdot\mathbf{y}\neq 0$.

key with a matrix $\mathbf{Y}$ specifying a linear space $\ker(\mathbf{Y})$. Decryption is possible whenever

$$(\mathbf{x}_0+\mathrm{span}(\mathbf{X}))\cap\ker(\mathbf{Y})\neq\emptyset$$

There is a generic transformation that allows us to handle affine spaces for secret keys starting from a construction for linear spaces (see Appendix A).

The starting point of our construction is the following DBDH-based spatial encryption scheme of Zhou and Cao [20], which corresponds to the special case where $\mathbf{X}$ is the all-zeroes matrix, so that decryption is possible iff $\mathbf{x}_0^\top\mathbf{Y}=\mathbf{0}$.

$$\begin{aligned}
\mathrm{MPK} &:= \Big(\ \mathbb{G}, e(g,g)^{\alpha}, g, g^{\mathbf{w}}, g^{\beta}\ \Big)\\
\mathrm{CT}_{\mathbf{x}_0} &:= \Big(\ g^{s},\ g^{(\beta\mathbf{x}_0+\mathbf{w})s},\ e(g,g)^{\alpha s}\cdot m\ \Big).\\
\mathrm{SK}_{\mathbf{Y}} &:= \Big(\ g^{\alpha-\mathbf{w}^\top\mathbf{Y}\mathbf{r}},\ g^{\mathbf{Y}\mathbf{r}}\ \Big).
\end{aligned}$$

Our first idea is to add $g^{\beta\mathbf{X}s}$ to the ciphertext, which would allow the decryptor to "delegate" the ciphertext to any vector in the affine space $\mathbf{x}_0+\mathrm{span}(\mathbf{X})$. This turns out to be completely insecure; one way to see this is that an adversary can take linear combinations of the rows in $\mathbf{X}$ instead of the columns, since the term $g^{\beta\mathbf{X}s}$ is insensitive to the rows or the columns of $\mathbf{X}$. Hamburg's DSE scheme [14] breaks this asymmetry by "compressing" $g^{\beta\mathbf{X}s}$ using a random linear combination of the rows (that is, β is replaced by a random vector $\mathbf{b}$); the ensuing construction has a structure similar to the HIBE scheme in [7] and we only know how to prove security under a stronger q-type assumption.

Our construction. We replace the scalar β in the spatial encryption scheme with a random $n\times n$ matrix $\mathbf{B}$, thereby breaking asymmetry while avoiding "compression":

$$\begin{aligned}
\mathrm{MPK} &:= \big(\ \mathbb{G}, e(g,g)^{\alpha}, g, g^{\mathbf{w}}, g^{\mathbf{B}}\ \big)\\
\mathrm{CT}_{(\mathbf{x}_0,\mathbf{X})} &:= \Big(\ g^{s},\ g^{(\boxed{\mathbf{B}^\top\mathbf{x}_0}+\mathbf{w})s},\ g^{\boxed{\mathbf{B}^\top\mathbf{X}}s},\ e(g,g)^{\alpha s}\cdot m\ \Big)\\
\mathrm{SK}_{\mathbf{Y}} &:= \Big(\ g^{\alpha-\mathbf{w}^\top\boxed{\mathbf{B}^{-1}\mathbf{Y}}\mathbf{r}},\ g^{\boxed{\mathbf{B}^{-1}\mathbf{Y}}\mathbf{r}}\ \Big)
\end{aligned}$$

To simulate the secret keys, we rely crucially on our new algebraic characterization in Lemma 1.

2 Preliminaries

Notation. We denote by $s \leftarrow_{\mathrm{R}} S$ the fact that s is picked uniformly at random from a finite set S and by $x, y, z \leftarrow_{\mathrm{R}} S$ that all x, y, z are picked independently and uniformly at random from S. By PPT, we denote a probabilistic polynomial-time algorithm. Throughout, we use 1^λ as the security parameter. We use $\cdot$ to denote multiplication (or group operation) as well as componentwise multiplication. We use lower case boldface to denote (column) vectors over scalars and upper case boldface to denote vectors of group elements as well as matrices. Given two vectors $\mathbf{x} = (x_1, x_2, \ldots), \mathbf{y} = (y_1, y_2, \ldots)$ over scalars, we use $\langle \mathbf{x}, \mathbf{y} \rangle$ to denote the standard dot product $\mathbf{x}^\top \mathbf{y}$. Given a group element g, we write $g^{\mathbf{x}}$ to denote $(g^{x_1}, g^{x_2}, \ldots)$; we define $g^{\mathbf{A}}$ where $\mathbf{A}$ is a matrix in an analogous way. Note that given a matrix of group elements $g^{\mathbf{A}}$, and a matrix $\mathbf{B}$ of "exponents", one can efficiently compute $g^{\mathbf{AB}}$; we will also denote this computation by $(g^{\mathbf{A}})^{\mathbf{B}}$.

Linear algebra. Given an $n \times d$ matrix $\mathbf{A}$ over $\mathbb{Z}_p$, we write $\mathrm{span}(\mathbf{A})$ to denote the linear space $\{\mathbf{Au} : \mathbf{u} \in \mathbb{Z}_p^d\} \subseteq \mathbb{Z}_p^n$ spanned by the columns of $\mathbf{A}$, and we write $\ker(\mathbf{A})$ to denote the linear space $\{\mathbf{x} : \mathbf{x}^\top \mathbf{A} = \mathbf{0}\} \subseteq \mathbb{Z}_p^n$ corresponding to the kernel of the column span of $\mathbf{A}$.

2.1 Doubly-Spatial Encryption

A DSE scheme consists of five algorithms ($\mathsf{Setup}, \mathsf{Enc}, \mathsf{KeyGen}, \mathsf{Dec}, \mathsf{KeyDel}$):

$\mathsf{Setup}(1^\lambda, 1^n) \rightarrow (\textsc{mpk}, \textsc{msk})$. The setup algorithm takes in a security parameter 1^λ, and a dimension parameter 1^n. It outputs public parameters MPK and a master secret key MSK.

$\mathsf{Enc}(\textsc{mpk}, (\mathbf{x}_0, \mathbf{X}), m) \rightarrow \textsc{ct}_{(\mathbf{x}_0, \mathbf{X})}$. The encryption algorithm takes in the public parameters MPK, a vector matrix pair $(\mathbf{x}_0, \mathbf{X})$, and a message m. It outputs a ciphertext $\textsc{ct}_{(\mathbf{x}_0, \mathbf{X})}$.

$\mathsf{KeyGen}(\textsc{mpk}, \textsc{msk}, \mathbf{Y}) \rightarrow \textsc{sk}_{\mathbf{Y}}$. The key generation algorithm takes in the public parameters MPK, the master secret key MSK, and a matrix $\mathbf{Y}$. It outputs a secret key $\textsc{sk}_{\mathbf{Y}}$.

$\mathsf{Dec}(\textsc{mpk}, \textsc{sk}_{\mathbf{Y}}, \textsc{ct}_{(\mathbf{x}_0, \mathbf{X})}) \rightarrow m$. The decryption algorithm takes in the public parameters MPK, a secret key $\textsc{sk}_{\mathbf{Y}}$ for $\mathbf{Y}$, and a ciphertext $\textsc{ct}_{(\mathbf{x}_0, \mathbf{X})}$ encrypted under $(\mathbf{x}_0, \mathbf{X})$. It outputs a message m if $(\mathbf{x}_0 + \mathrm{span}(\mathbf{X})) \cap \ker(\mathbf{Y}) \neq \emptyset$.

$\mathsf{KeyDel}(\textsc{mpk}, \textsc{sk}_{\mathbf{Y}}, \mathbf{Y}') \rightarrow \textsc{sk}_{\mathbf{Y}'}$. The key delegation algorithm takes in the public parameters MPK, a secret key $\textsc{sk}_{\mathbf{Y}}$, and a matrix $\mathbf{Y}'$, where $\mathrm{span}(\mathbf{Y}') \subseteq \mathrm{span}(\mathbf{Y})$. It outputs a secret key $\textsc{sk}_{\mathbf{Y}'}$.

Correctness. For all $(\textsc{mpk}, \textsc{msk}) \leftarrow \mathsf{Setup}(1^\lambda, 1^n)$, all vector matrix pairs $(\mathbf{x}_0, \mathbf{X})$, all messages m, all decryption keys $\textsc{sk}_{\mathbf{Y}}$, all $(\mathbf{x}_0, \mathbf{X})$ such that $(\mathbf{x}_0 + \mathrm{span}(\mathbf{X})) \cap \ker(\mathbf{Y}) \neq \emptyset$, we have

$$\Pr[\mathsf{Dec}(\textsc{mpk}, \textsc{sk}_{\mathbf{Y}}, \mathsf{Enc}(\textsc{mpk}, (\mathbf{x}_0, \mathbf{X}), m)) = m] = 1.$$

Delegation. We require that delegation is independent of the path taken; that is, if $\mathrm{span}(\mathbf{Y}') \subseteq \mathrm{span}(\mathbf{Y})$, then the following distributions are identical:

$$\{\textsc{sk}_{\mathbf{Y}}, \mathsf{KeyDel}(\textsc{mpk}, \textsc{sk}_{\mathbf{Y}}, \mathbf{Y}')\} \quad \text{and} \quad \{\textsc{sk}_{\mathbf{Y}}, \mathsf{KeyGen}(\textsc{mpk}, \textsc{msk}, \mathbf{Y}')\}$$

2.2 Selective Security Model

We now give the notion of *selective* security for DSE. Briefly, the adversary specifies the challenge affine space before it sees the public parameters. The security game is defined by the following experiment, played by a challenger and an adversary $\mathcal{A}$.

Challenge Space. The adversary $\mathcal{A}$ gives the challenger the dimension parameter 1^n and challenge vector matrix pair $(\mathbf{x}_0^*, \mathbf{X})$.

Setup. The challenger runs the setup algorithm to generate $(\textsc{mpk}, \textsc{msk})$. It gives $\textsc{mpk}$ to the adversary $\mathcal{A}$.

Phase 1. The adversary $\mathcal{A}$ adaptively requests keys for any matrix $\mathbf{Y}$ of its choice with the restriction that $(\mathbf{x}_0^* + \mathrm{span}(\mathbf{X})) \cap \ker(\mathbf{Y}) = \emptyset$. The challenger $\mathcal{C}$ responds with the corresponding secret key $\textsc{sk}_{\mathbf{Y}}$, which it generates by running $\mathsf{KeyGen}(\textsc{mpk}, \textsc{msk}, \mathbf{Y})$. Because of our restriction on delegation, the returned $\textsc{sk}_{\mathbf{Y}}$ is independent of the path taken.

Challenge Ciphertext. The adversary submits two messages m_0 and m_1 of equal length. $\mathcal{C}$ picks $\beta \leftarrow_{\mathrm{R}} \{0,1\}$ and encrypts m_β under $(\mathbf{x}_0^*, \mathbf{X})$ by running the encryption algorithm. It sends the ciphertext to the adversary $\mathcal{A}$.

Phase 2. $\mathcal{A}$ continues to issue key queries as in **Phase 1**.

Guess. The adversary $\mathcal{A}$ must output a guess β' for β.

The advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathrm{DSE}}(\lambda)$ of an adversary $\mathcal{A}$ is defined to be $\Pr[\beta' = \beta] - 1/2$.

Definition 1. *A DSE scheme is* selectively secure *if all PPT adversaries achieve at most a negligible advantage in the above security game.*

2.3 Computational Assumptions

We now briefly recall bilinear pairing groups and then state the decisional bilinear Diffie-Hellman (DBDH) assumption that are required in our security proof.

A generator $\mathcal{G}$ which takes as input a security parameter 1^λ and outputs a description $\mathbb{G} := (p, G, G_T, e)$, where p is a prime of $\Theta(\lambda)$ bits, G and G_T are cyclic groups of order p, and $e : G \times G \rightarrow G_T$ is a non-degenerate bilinear map. We require that the group operations in G and G_T as well the bilinear map e are computable in deterministic polynomial time with respect to λ. Furthermore, the group descriptions of G and G_T include generators of the respective cyclic groups.

Assumption 1 (DBDH: Decisional Bilinear Diffie-Hellman Assumption) *Given a group generator $\mathcal{G}(1^\lambda)$, we define the following distribution:*

$$\begin{aligned}
&\mathbb{G} := (p, G, G_T, g, e) \leftarrow_{\mathrm{R}} \mathcal{G}(1^\lambda),\\
&a, b, s, z \leftarrow_{\mathrm{R}} \mathbb{Z}_p,\\
&T_0 := g^{abs},\ T_1 := g^{abs+z},\\
&D := (\mathbb{G}; g^a, g^b, g^s).
\end{aligned}$$

We assume that for any PPT algorithm $\mathcal{A}$ (with output in $\{0,1\}$),

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{DBDH}}(\lambda) := |\Pr[\mathcal{A}(D,T_0)=1] - \Pr[\mathcal{A}(D,T_1)=1]|$$

is negligible in the security parameter λ.

2.4 Algebraic Characterization for DSE

Next, we present a novel algebraic characterization of NO instances for the DSE functionality, which we use crucially in the proof of security.

Lemma 1. *Fix $(\mathbf{x}_0, \mathbf{X}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^{n\times d}$ and $\mathbf{Y} \in \mathbb{Z}_p^{n\times \ell}$. If*

$$(\mathbf{x}_0 + \mathrm{span}(\mathbf{X})) \cap \ker(\mathbf{Y}) = \emptyset,$$

then we can efficiently compute $\mathbf{z} \in \mathbb{Z}_p^\ell$ such that

$$\mathbf{x}_0^\top \mathbf{Y}\mathbf{z} = 1 \quad \textit{and} \quad \mathbf{X}^\top \mathbf{Y}\mathbf{z} = \mathbf{0}.$$

Remark 1. Observe that the converse is also true. Suppose such a $\mathbf{z}$ exists. Then for all $\mathbf{x}' = \mathbf{x}_0 + \mathbf{X}\mathbf{u} \in (\mathbf{x}_0 + \mathrm{span}(\mathbf{X}))$, we have $(\mathbf{x}')^\top \mathbf{Y}\mathbf{z} = \mathbf{x}_0^\top \mathbf{Y}\mathbf{z} + \mathbf{u}^\top \mathbf{X}^\top \mathbf{Y}\mathbf{z} = 1$, which means $\mathbf{x}' \notin \ker(\mathbf{Y})$. This implies $(\mathbf{x}_0 + \mathrm{span}(\mathbf{X})) \cap \ker(\mathbf{Y}) = \emptyset$.

Proof. Our goal is to find a column vector $\mathbf{z} \in \mathbb{Z}_p^\ell$ such that

$$(\mathbf{x}_0 \| \mathbf{X})^\top \mathbf{Y}\mathbf{z} = \mathbf{e}_1$$

If a solution exists, we can always find it efficiently using Gaussian elimination. Suppose on the contrary that a solution does not exist. Then, there must exist a (column) vector $\mathbf{u} \in \mathbb{Z}_p^{d+1}$ such that

$$\mathbf{u}^\top (\mathbf{x}_0 \| \mathbf{X})^\top \mathbf{Y} = \mathbf{0} \quad \text{and} \quad \mathbf{u}^\top \mathbf{e}_1 = 1$$

Therefore,

$$(\mathbf{x}_0 \| \mathbf{X})\mathbf{u} \in \ker(\mathbf{Y}) \quad \text{and} \quad (\mathbf{x}_0 \| \mathbf{X})\mathbf{u} \in (\mathbf{x}_0 + \mathrm{span}(\mathbf{X})).$$

This means

$$(\mathbf{x}_0 + \mathrm{span}(\mathbf{X})) \cap \ker(\mathbf{Y}) \neq \emptyset,$$

a contradiction. □

3 Doubly-Spatial Encryption

3.1 Construction

First, we describe the scheme without delegation.

- $\mathsf{Setup}(1^\lambda, 1^n)$: On input $(1^\lambda, 1^n)$, generate $\mathbb{G} := (p, G, G_T, e) \leftarrow_{\mathrm{R}} \mathcal{G}(1^\lambda)$, pick $\alpha \leftarrow_{\mathrm{R}} \mathbb{Z}_p$, $\mathbf{w} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^n$, $\mathbf{B} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{n\times n}$, and output

$$\mathrm{MPK} := \big(\, \mathbb{G}; e(g,g)^\alpha, g, g^{\mathbf{w}}, g^{\mathbf{B}} \,\big) \in G_T \times G \times G^n \times G^{n\times n}$$

and

$$\text{MSK} := \big(\ \alpha, \mathbf{w}, \mathbf{B}^{-1}\ \big) \in \mathbb{Z}_p \times \mathbb{Z}_p^n \times \mathbb{Z}_p^{n\times n}.$$

- $\mathsf{Enc}(\text{MPK}, (\mathbf{x}_0, \mathbf{X}), m)$: On input $(\mathbf{x}_0, \mathbf{X}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^{n\times d}$, and message $m \in G_T$, pick $s \leftarrow_{\text{R}} \mathbb{Z}_p$ and output

$$\text{CT}_{(\mathbf{x}_0,\mathbf{X})} := \Big(\ C_0 := g^s,\ \mathbf{C}_1 := g^{(\mathbf{B}^\top \mathbf{x}_0 + \mathbf{w})s},\ \mathbf{C}_2 := g^{\mathbf{B}^\top \mathbf{X} s},\ C' := e(g,g)^{\alpha s} \cdot m\ \Big)$$
$$\in G \times G^n \times G^{n\times d} \times G_T.$$

- $\mathsf{KeyGen}(\text{MPK}, \text{MSK}, \mathbf{Y})$: On input $\mathbf{Y} \in \mathbb{Z}_p^{n\times \ell}$, pick $\mathbf{r} \leftarrow_{\text{R}} \mathbb{Z}_p^\ell$ and output

$$\text{SK}_{\mathbf{Y}} := \Big(\ K_0 := g^{\alpha - \langle \mathbf{w}, \mathbf{B}^{-1}\mathbf{Y}\mathbf{r}\rangle},\ \mathbf{K}_1 := g^{\mathbf{B}^{-1}\mathbf{Y}\mathbf{r}}\ \Big) \in G \times G^n.$$

- $\mathsf{Dec}(\text{MPK}, \text{SK}_{\mathbf{Y}}, \text{CT}_{(\mathbf{x}_0,\mathbf{X})})$: If $(\mathbf{x}_0 + \text{span}(\mathbf{X})) \cap \ker(\mathbf{Y}) \neq \emptyset$, first compute $\mathbf{u} \in \mathbb{Z}_p^d$ such that

$$\mathbf{x}' := \mathbf{x}_0 + \mathbf{X} \cdot \mathbf{u} \in \ker(\mathbf{Y})$$

  Parse the ciphertext as $(C_0, \mathbf{C}_1, \mathbf{C}_2, C')$ and compute

$$e(g,g)^{\alpha s} \leftarrow e(C_0, K_0) \cdot e(\mathbf{C}_1 \cdot \mathbf{C}_2^{\mathbf{u}}, \mathbf{K}_1).$$

  Recover the message as $m \leftarrow C'/e(g,g)^{\alpha s} \in G_T$.

Claim. For all $\mathbf{x}, \mathbf{y}$, we have $\langle \mathbf{B}^\top \mathbf{x}, \mathbf{B}^{-1}\mathbf{y}\rangle = \langle \mathbf{x}, \mathbf{y}\rangle$.

Correctness. Fix $(\mathbf{x}_0, \mathbf{X})$ and $\mathbf{Y}$ such that $(\mathbf{x}_0 + \text{span}(\mathbf{X})) \cap \ker(\mathbf{Y}) \neq \emptyset$. Let $(\mathbf{u}, \mathbf{x}')$ be the vectors computed by $\mathsf{Dec}(\text{MPK}, \text{SK}_{\mathbf{Y}}, \text{CT}_{(\mathbf{x}_0,\mathbf{X})})$ so that

$$\mathbf{x}' = \mathbf{x}_0 + \mathbf{X}\mathbf{u} \quad \text{and} \quad \mathbf{x}'^\top \mathbf{Y} = \mathbf{0}$$

First, observe that

$$\begin{aligned} e(\mathbf{C}_1 \cdot \mathbf{C}_2^{\mathbf{u}}, \mathbf{K}_1) &= e(g^{(\mathbf{B}^\top \mathbf{x}_0 + \mathbf{w} + \mathbf{B}^\top \mathbf{X}\mathbf{u})s}, g^{\mathbf{B}^{-1}\mathbf{Y}\mathbf{r}}) \\ &= e(g^s, g^{\langle \mathbf{B}^\top \mathbf{x}_0 + \mathbf{w} + \mathbf{B}^\top \mathbf{X}\mathbf{u}, \mathbf{B}^{-1}\mathbf{Y}\mathbf{r}\rangle}) \end{aligned}$$

We then compute the exponent on the second term as follows:

$$\begin{aligned} \langle \mathbf{B}^\top \mathbf{x}_0 + \mathbf{w} + \mathbf{B}^\top \mathbf{X}\mathbf{u}, \mathbf{B}^{-1}\mathbf{Y}\mathbf{r}\rangle &= \langle \mathbf{B}^\top \mathbf{x}' + \mathbf{w}, \mathbf{B}^{-1}\mathbf{Y}\mathbf{r}\rangle \\ &= \langle \mathbf{B}^\top \mathbf{x}', \mathbf{B}^{-1}\mathbf{Y}\mathbf{r}\rangle + \langle \mathbf{w}, \mathbf{B}^{-1}\mathbf{Y}\mathbf{r}\rangle \\ &= \langle \mathbf{x}', \mathbf{Y}\mathbf{r}\rangle + \langle \mathbf{w}, \mathbf{B}^{-1}\mathbf{Y}\mathbf{r}\rangle \\ &= \langle \mathbf{w}, \mathbf{B}^{-1}\mathbf{Y}\mathbf{r}\rangle \\ \implies \quad e(\mathbf{C}_1 \cdot \mathbf{C}_2^{\mathbf{u}}, \mathbf{K}_1) &= e(g^s, g^{\langle \mathbf{w}, \mathbf{B}^{-1}\mathbf{Y}\mathbf{r}\rangle}) \end{aligned}$$

Therefore,

$$\begin{aligned} e(C_0, K_0) \cdot e(\mathbf{C}_1 \cdot \mathbf{C}_2^{\mathbf{u}}, \mathbf{K}_1) &= e(g^s, g^{\alpha - \langle \mathbf{w}, \mathbf{B}^{-1}\mathbf{Y}\mathbf{r}\rangle}) \cdot e(g^s, g^{\langle \mathbf{w}, \mathbf{B}^{-1}\mathbf{Y}\mathbf{r}\rangle}) \\ &= e(g,g)^{\alpha s}. \end{aligned}$$

Correctness follows readily.

3.2 Proof of DSE Security

We prove the following theorem:

Theorem 1. *Under DBDH assumption (described in Section 2.3), our DSE scheme defined in Section 3.1 is selectively secure (in the sense of Definition 2.2). More precisely, for any adversary $\mathcal{A}$ against the DSE scheme, there exists an adversary $\mathcal{B}$ such that*

$$\mathsf{Adv}^{\text{DSE}}_{\mathcal{A}}(\lambda) \le \mathsf{Adv}^{\text{DBDH}}_{\mathcal{B}}(\lambda) + 1/p.$$

and

$$\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A}) + q \cdot \text{poly}(\lambda, n),$$

where $\text{poly}(\lambda, n)$ *is independent of* $\mathsf{Time}(\mathcal{A})$.

Overview of proof. Fix the selective challenge $(\mathbf{x}_0^*, \mathbf{X})$. Recall that the challenge ciphertext is of the form

$$\Big(\, g^s,\ g^{(\mathbf{B}^\top \mathbf{x}_0^* + \mathbf{w})s},\ g^{\mathbf{B}^\top \mathbf{X} s},\ \boxed{e(g,g)^{\alpha s} \cdot m_\beta}\,\Big) \quad \text{or} \quad \Big(\, g^s,\ g^{(\mathbf{B}^\top \mathbf{x}_0^* + \mathbf{w})s},\ g^{\mathbf{B}^\top \mathbf{X} s},\ \boxed{e(g,g)^{\alpha s} \cdot \text{random}}\,\Big)$$

Following [4], we implicitly set $\alpha := ab$ where (g, g^a, g^b, g^s) are provided in the DBDH assumption. Next, we pick $\bar{\mathbf{X}} \in \mathbb{Z}_p^{n \times (n-d)}$ so that $(\mathbf{X} \| \bar{\mathbf{X}})$ is a full rank matrix. Intuitively, we program $\mathbf{B}$ so that know

$$\mathbf{B}^\top \mathbf{X} \quad \text{and} \quad a^{-1} \cdot \mathbf{B}^\top \bar{\mathbf{X}}$$

We need the first term to simulate the challenge ciphertext, whereas knowing the second term will help us answer secret key queries later by 'canceling out' terms we do not know how to compute. In addition, we pick $\tilde{\mathbf{w}} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^n$ and implicitly set

$$\mathbf{B}^\top \mathbf{x}_0^* + \mathbf{w} := \tilde{\mathbf{w}}$$

Simulating the public parameters and the challenge ciphertext is straight-forward.

The main challenge lies in simulating the secret key

$$\text{SK}_{\mathbf{Y}} = \Big(\, g^{\alpha - \langle \mathbf{w}, \mathbf{B}^{-1} \mathbf{Y} \mathbf{r} \rangle},\ g^{\mathbf{B}^{-1} \mathbf{Y} \mathbf{r}} \,\Big),$$

which we may rewrite in terms of ab and $\tilde{\mathbf{w}}$ as

$$\Big(\, g^{ab + \langle \mathbf{x}_0^*, \mathbf{Y}\mathbf{r} \rangle - \langle \tilde{\mathbf{w}}, \mathbf{B}^{-1} \mathbf{Y} \mathbf{r} \rangle},\ g^{\mathbf{B}^{-1} \mathbf{Y} \mathbf{r}} \,\Big).$$

With some algebraic manipulation upon replacing $\mathbf{B}$ with terms we know (in particular, that we know $a^{-1} \cdot \mathbf{B}^\top \bar{\mathbf{X}}$), it suffices to show how to simulate

$$\Big(\, g^{ab + \langle \mathbf{x}_0^*, \mathbf{Y}\mathbf{r} \rangle},\ g^{\mathbf{X}^\top \mathbf{Y} \mathbf{r}},\ g^{a^{-1} \bar{\mathbf{X}}^\top \mathbf{Y} \mathbf{r}} \,\Big).$$

To achieve this, we program $\mathbf{r}$ to cancel out both ab and a^{-1}. Since $(\mathbf{x}_0^* + \mathrm{span}(\mathbf{X})) \cap \ker(\mathbf{Y}) = \emptyset$, we can compute $\mathbf{z} \in \mathbb{Z}_p^\ell$ such that $(\mathbf{x}_0^*)^\top \mathbf{Y}\mathbf{z} = 1$ and $\mathbf{X}^\top \mathbf{Y}\mathbf{z} = \mathbf{0}$ (c.f. Lemma 1). Then, we proceed as follows:

- we pick $\tilde{\mathbf{r}} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^\ell$ and implicitly set $\mathbf{r} := a\tilde{\mathbf{r}} - ab\mathbf{z}$;
- we can cancel out ab by using $\langle \mathbf{x}_0^*, \mathbf{Y}\mathbf{r}\rangle$, namely

$$\begin{aligned} ab + \langle \mathbf{x}_0^*, \mathbf{Y}\mathbf{r}\rangle &= ab + \langle \mathbf{x}_0^*, \mathbf{Y}(a\tilde{\mathbf{r}} - ab\mathbf{z})\rangle \\ &= ab + a\langle \mathbf{x}_0^*, \mathbf{Y}\tilde{\mathbf{r}}\rangle - ab\langle \mathbf{x}_0^*, \mathbf{Y}\mathbf{z}\rangle \\ &= a\langle \mathbf{x}_0^*, \mathbf{Y}\tilde{\mathbf{r}}\rangle. \end{aligned}$$

- observe that $\mathbf{X}^\top \mathbf{Y}\mathbf{r} = a\mathbf{X}^\top \mathbf{Y}\tilde{\mathbf{r}}$ and $a^{-1}\bar{\mathbf{X}}^\top \mathbf{Y}\mathbf{r} = \bar{\mathbf{X}}^\top \mathbf{Y}\tilde{\mathbf{r}} - b\bar{\mathbf{X}}^\top \mathbf{Y}\mathbf{z}$.

That is, we can simulate the expression above as:

$$\Big(\ (g^a)^{\langle \mathbf{x}_0^*, \mathbf{Y}\tilde{\mathbf{r}}\rangle},\ (g^a)^{\mathbf{X}^\top \mathbf{Y}\tilde{\mathbf{r}}},\ g^{\bar{\mathbf{X}}^\top \mathbf{Y}\tilde{\mathbf{r}}} \cdot (g^b)^{-\bar{\mathbf{X}}^\top \mathbf{Y}\mathbf{z}}\ \Big).$$

Proof. We construct an adversary $\mathcal{B}$ for DBDH assumption using $\mathcal{A}$. Recall that in DBDH assumption, the adversary is given $D := (\mathbb{G}; g, g^a, g^b, g^s)$, along with T, where T equals $e(g,g)^{abs}$ or is drawn uniformly from G_T. Here, we assume that $a \leftarrow_{\mathrm{R}} \mathbb{Z}_p^*$, which yields a $1/p$ negligible difference from DBDH assumption in the advantage; $\mathcal{B}$ proceeds as follows:

Setup. On input selective challenge $(\mathbf{x}_0^*, \mathbf{X})$, pick $\bar{\mathbf{X}} \in \mathbb{Z}_p^{n\times(n-d)}$ so that $(\mathbf{X}\|\bar{\mathbf{X}})$ is a full rank matrix. Intuitively, we want to pick a random full rank $\mathbf{B}$ so that we can compute

$$\mathbf{B}^\top \mathbf{X} \quad \text{and} \quad a^{-1} \cdot \mathbf{B}^\top \bar{\mathbf{X}}$$

We will need to know the first term to simulate the challenge ciphertext, whereas knowing the second term will help us answer secret key queries later by 'canceling out' terms we do not know how to compute. To achieve this, we pick a random full rank matrix $\mathbf{Z}\|\bar{\mathbf{Z}} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{n\times n}$ and implicitly set

$$\mathbf{B}^\top \mathbf{X} = \mathbf{Z} \quad \text{and} \quad \mathbf{B}^\top \bar{\mathbf{X}} = a\bar{\mathbf{Z}},$$

that is,

$$\mathbf{B}^\top := (\mathbf{Z}\|a\bar{\mathbf{Z}})(\mathbf{X}\|\bar{\mathbf{X}})^{-1} \quad \text{and} \quad \mathbf{B}^{-1} := ((\mathbf{Z}\|\bar{\mathbf{Z}})^{-1})^\top (\mathbf{X}\|a^{-1}\bar{\mathbf{X}})^\top.$$

Observe that we can compute $g^{\mathbf{B}^\top}$ as

$$(g^{\mathbf{Z}}\|(g^a)^{\bar{\mathbf{Z}}})^{(\mathbf{X}\|\bar{\mathbf{X}})^{-1}}.$$

In addition, we pick $\tilde{\mathbf{w}} \leftarrow \mathbb{Z}_p^n$ and implicitly set

$$\mathbf{w} := -\mathbf{B}^\top \mathbf{x}_0^* + \tilde{\mathbf{w}}$$

Note that we can then compute $g^{\mathbf{w}}$ as $(g^{\mathbf{B}^\top})^{-\mathbf{x}_0^*} \cdot g^{\tilde{\mathbf{w}}}$. Finally, $\mathcal{B}$ implicitly sets $\alpha := ab$ and outputs

$$\text{MPK} := (\ \mathbb{G}; e(g^a, g^b), g, g^{\mathbf{w}}, g^{\mathbf{B}}\ ).$$

Key Queries. On input $\mathbf{Y} \in \mathbb{Z}_p^{n \times \ell}$, where $(\mathbf{x}_0^* + \mathrm{span}(\mathbf{X})) \cap \ker(\mathbf{Y}) = \emptyset$, recall that

$$\textsc{sk}_{\mathbf{Y}} := \Big(K_0 := g^{\alpha - \langle \mathbf{w}, \mathbf{B}^{-1}\mathbf{Y}\mathbf{r} \rangle},\ \mathbf{K}_1 := g^{\mathbf{B}^{-1}\mathbf{Y}\mathbf{r}} \Big).$$

which we may rewrite in terms of ab and $\tilde{\mathbf{w}}$ as

$$\Big(g^{ab + \langle \mathbf{x}_0^*, \mathbf{Y}\mathbf{r} \rangle - \langle \tilde{\mathbf{w}}, \mathbf{B}^{-1}\mathbf{Y}\mathbf{r} \rangle},\ g^{\mathbf{B}^{-1}\mathbf{Y}\mathbf{r}} \Big).$$

First, we show how to compute the following expression

$$\Big(g^{ab + \langle \mathbf{x}_0^*, \mathbf{Y}\mathbf{r} \rangle},\ g^{\mathbf{X}^\top \mathbf{Y}\mathbf{r}},\ g^{a^{-1}\bar{\mathbf{X}}^\top \mathbf{Y}\mathbf{r}} \Big) \qquad (*).$$

To do this, the adversary $\mathcal{B}$ picks $\tilde{\mathbf{r}} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^\ell$ and implicitly sets

$$\mathbf{r} := a\tilde{\mathbf{r}} - ab\mathbf{z}$$

where $\mathbf{z}$ is computed as in Lemma 1 so that $(\mathbf{x}_0^*)^\top \mathbf{Y}\mathbf{z} = 1$ and $\mathbf{X}^\top \mathbf{Y}\mathbf{z} = \mathbf{0}$. Now, observe that

$$\begin{aligned} ab + \langle \mathbf{x}_0^*, \mathbf{Y}\mathbf{r} \rangle &= ab + \langle \mathbf{x}_0^*, \mathbf{Y}(a\tilde{\mathbf{r}} - ab\mathbf{z}) \rangle \\ &= ab + a\langle \mathbf{x}_0^*, \mathbf{Y}\tilde{\mathbf{r}} \rangle - ab\langle \mathbf{x}_0^*, \mathbf{Y}\mathbf{z} \rangle \\ &= a\langle \mathbf{x}_0^*, \mathbf{Y}\tilde{\mathbf{r}} \rangle \end{aligned}$$

where in the last equality, we use the fact that $(\mathbf{x}_0^*)^\top \mathbf{Y}\mathbf{z} = 1$. In addition, we have

$$\begin{aligned} \mathbf{X}^\top \mathbf{Y}\mathbf{r} &= \mathbf{X}^\top \mathbf{Y}(a\tilde{\mathbf{r}} - ab\mathbf{z}) = \mathbf{X}^\top \mathbf{Y}\tilde{\mathbf{r}} \\ a^{-1}\bar{\mathbf{X}}^\top \mathbf{Y}\mathbf{r} &= a^{-1}\bar{\mathbf{X}}^\top \mathbf{Y}(a\tilde{\mathbf{r}} - ab\mathbf{z}) = \bar{\mathbf{X}}^\top \mathbf{Y}\tilde{\mathbf{r}} - b\bar{\mathbf{X}}^\top \mathbf{Y}\mathbf{z}. \end{aligned}$$

That is, given g, g^a, g^b along with $\mathbf{x}_0^*, \tilde{\mathbf{r}}, \mathbf{z}, \mathbf{X}, \bar{\mathbf{X}}, \mathbf{Y}$, we can compute the expression $(*)$ as:

$$\Big((g^a)^{\langle \mathbf{x}_0^*, \mathbf{Y}\tilde{\mathbf{r}} \rangle},\ (g^a)^{\mathbf{X}^\top \mathbf{Y}\tilde{\mathbf{r}}},\ g^{\bar{\mathbf{X}}^\top \mathbf{Y}\tilde{\mathbf{r}}} \cdot (g^b)^{-\bar{\mathbf{X}}^\top \mathbf{Y}\mathbf{z}} \Big).$$

Next, we show how to simulate $\textsc{sk}_{\mathbf{Y}}$ using the expression $(*)$. Note that

$$K_0 = g^{ab + \langle \mathbf{x}_0^*, \mathbf{Y}\mathbf{r} \rangle} \cdot g^{-\langle \tilde{\mathbf{w}}, \mathbf{B}^{-1}\mathbf{Y}\mathbf{r} \rangle},$$

where we can compute $g^{\langle \tilde{\mathbf{w}}, \mathbf{B}^{-1}\mathbf{Y}\mathbf{r} \rangle}$ given $\mathbf{K}_1 = g^{\mathbf{B}^{-1}\mathbf{Y}\mathbf{r}}$ and $\tilde{\mathbf{w}}$ by computing a dot product in the exponent. Thus, it suffices to show how to compute $\mathbf{K}_1$ using $g^{\mathbf{X}^\top \mathbf{Y}\mathbf{r}}, g^{a^{-1}\tilde{\mathbf{X}}^\top \mathbf{Y}\mathbf{r}}$. Recall that

$$\mathbf{B}^{-1} = ((\mathbf{Z} \| \bar{\mathbf{Z}})^{-1})^\top (\mathbf{X} \| a^{-1}\bar{\mathbf{X}})^\top,$$

we have

$$\mathbf{B}^{-1}\mathbf{Y}\mathbf{r} = ((\mathbf{Z} \| \bar{\mathbf{Z}})^{-1})^\top \binom{\mathbf{X}^\top \mathbf{Y}\mathbf{r}}{a^{-1}\bar{\mathbf{X}}^\top \mathbf{Y}\mathbf{r}}.$$

Written this way, it is easy to see that given $g^{\mathbf{X}^\top \mathbf{Y}\mathbf{r}}, g^{a^{-1}\tilde{\mathbf{X}}^\top \mathbf{Y}\mathbf{r}}$ along with $\mathbf{Z}, \bar{\mathbf{Z}}$, we can compute $\mathbf{K}_1 = g^{\mathbf{B}^{-1}\mathbf{Y}\mathbf{r}}$.

Challenge Ciphertext. Upon receiving two equal length messages m_0 and m_1 from $\mathcal{A}$, $\mathcal{B}$ picks $\beta \leftarrow_{\mathrm{R}} \{0,1\}$ and outputs the challenge ciphertext as:

$$\mathrm{CT}_{(\mathbf{x}_0^*, \mathbf{X})} := \big(\, C_0 := g^s,\ \mathbf{C}_1 := g^{\tilde{\mathbf{w}} s},\ \mathbf{C}_2 := g^{\mathbf{Z} s},\ C' := T \cdot m_\beta \,\big)\,.$$

Now, if T equals $e(g,g)^{abs}$, this would indeed be a properly distributed encryption of m_β. On the other hand, if $T \leftarrow_{\mathrm{R}} G_T$, instead, then the challenge ciphertext is an encryption of a random message in G_T and therefore independent of β.

Guess. When $\mathcal{A}$ halts with output β', $\mathcal{B}$ outputs 1 if $\beta = \beta'$ and 0 otherwise.

We may therefore conclude that $\mathsf{Adv}_{\mathcal{A}}^{\mathrm{DSE}}(\lambda) \le \mathsf{Adv}_{\mathcal{B}}^{\mathrm{DBDH}}(\lambda) + 1/p$. □

3.3 Construction with Delegation

We describe how to support delegation. It suffices to modify Setup, and to add KeyDel.

- $\mathsf{Setup}(1^\lambda, 1^n)$: On input a dimensional parameter 1^n, generate $\mathbb{G} := (p, G, G_T, e) \leftarrow_{\mathrm{R}} \mathcal{G}(1^\lambda)$. Pick $\alpha, \leftarrow_{\mathrm{R}} \mathbb{Z}_p$, $\mathbf{w} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^n$, $\mathbf{B} \in \mathbb{Z}_p^{n \times n}$. $\boxed{\text{In addition, pick } \gamma \leftarrow_{\mathrm{R}} \mathbb{Z}_p^*.}$ Output

  $$\mathrm{MPK} := \left(\mathbb{G}; e(g,g)^\alpha, g, g^{\mathbf{w}}, g^{\mathbf{B}}, \boxed{g^{\gamma \mathbf{B}^{-1}}, g^{\gamma (\mathbf{B}^{-1})^\top \mathbf{w}}} \right) \in G_T \times G \times G^n \times G^{n \times n} \times \boxed{G^{n \times n} \times G^n}$$

  and

  $$\mathrm{MSK} := \big(\, \alpha, \mathbf{w}, \mathbf{B}^{-1} \,\big) \in \mathbb{Z}_p \times \mathbb{Z}_p^n \times \mathbb{Z}_p^{n \times n}.$$

- $\mathsf{KeyDel}(\mathrm{MPK}, \mathrm{SK}_{\mathbf{Y}}, \mathbf{Y}')$: On input $\mathrm{SK}_{\mathbf{Y}} := (K_0 := g^{\alpha - \langle \mathbf{w}, \mathbf{B}^{-1}\mathbf{Y}\mathbf{r}\rangle}, \mathbf{K}_1 := g^{\mathbf{B}^{-1}\mathbf{Y}\mathbf{r}}) \in G \times G^n$ and $\mathbf{Y}' \in \mathbb{Z}_p^{n \times \ell'}$, where $\mathrm{span}(\mathbf{Y}) \subseteq \mathrm{span}(\mathbf{Y}')$, pick $\tilde{\mathbf{r}} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{\ell'}$ and output

  $$\mathrm{SK}_{\mathbf{Y}'} := \left(\, K_0' := K_0 \cdot g^{-\gamma \langle \mathbf{w}, \mathbf{B}^{-1}\mathbf{Y}'\tilde{\mathbf{r}}\rangle},\ \mathbf{K}_1' := \mathbf{K}_1 \cdot g^{\gamma \mathbf{B}^{-1}\mathbf{Y}'\tilde{\mathbf{r}}} \,\right) \in G \times G^n.$$

  Note that $\gamma \langle \mathbf{w}, \mathbf{B}^{-1}\mathbf{Y}'\tilde{\mathbf{r}}\rangle = \langle \gamma (\mathbf{B}^{-1})^\top \mathbf{w}, \mathbf{Y}'\tilde{\mathbf{r}}\rangle$, so we can compute $g^{\gamma\langle \mathbf{w}, \mathbf{B}^{-1}\mathbf{Y}'\tilde{\mathbf{r}}\rangle}$ by computing a dot product of $g^{\gamma(\mathbf{B}^{-1})^\top \mathbf{w}}$ and $\mathbf{Y}'\tilde{\mathbf{r}}$ in the exponent.

Delegation. Fix $\mathbf{Y}$ and $\mathbf{Y}'$ such that $\mathrm{span}(\mathbf{Y}) \subseteq \mathrm{span}(\mathbf{Y}')$, which means we can efficiently compute a matrix $\mathbf{T} \in \mathbb{Z}_p^{\ell' \times \ell}$ such that $\mathbf{Y} = \mathbf{Y}'\mathbf{T}$. It suffices to the output $\mathrm{SK}_{\mathbf{Y}'} := (D_0', \mathbf{K}_1')$ from KeyDel is the same as that computed by KeyGen using a fresh random vector $\mathbf{r}' \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{\ell'}$, where

$$\mathbf{r} := \mathbf{T}\mathbf{r} + \gamma \tilde{\mathbf{r}},$$

Note that $\mathbf{r}'$ is indeed uniformly random from $\mathbb{Z}_p^{\ell'}$ (whenever $\gamma \neq 0$) since $\tilde{\mathbf{r}} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{\ell'}$. Now, observe that

$$\begin{array}{ll}
\begin{aligned}
K_0' &= K_0 \cdot g^{-\gamma\langle \mathbf{w}, \mathbf{B}^{-1}\mathbf{Y}'\tilde{\mathbf{r}}\rangle} \\
&= g^{\alpha - \langle \mathbf{w}, \mathbf{B}^{-1}\mathbf{Y}\mathbf{r}\rangle} \cdot g^{-\gamma\langle \mathbf{w}, \mathbf{B}^{-1}\mathbf{Y}'\tilde{\mathbf{r}}\rangle} \\
&= g^{\alpha - \langle \mathbf{w}, \mathbf{B}^{-1}\mathbf{Y}'(\mathbf{T}\mathbf{r})\rangle} \cdot g^{-\langle \mathbf{w}, \mathbf{B}^{-1}\mathbf{Y}'(\gamma\tilde{\mathbf{r}})\rangle} \\
&= g^{\alpha - \langle \mathbf{w}, \mathbf{B}^{-1}\mathbf{Y}'(\mathbf{T}\mathbf{r}+\gamma\tilde{\mathbf{r}})\rangle} \\
&= g^{\alpha - \langle \mathbf{w}, \mathbf{B}^{-1}\mathbf{Y}'\mathbf{r}'\rangle}
\end{aligned}
&
\begin{aligned}
\mathbf{K}_1' &= \mathbf{K}_1 \cdot g^{\mathbf{B}^{-1}\mathbf{Y}'\tilde{\mathbf{r}}} \\
&= g^{\mathbf{B}^{-1}\mathbf{Y}\mathbf{r}} \cdot g^{\gamma\mathbf{B}^{-1}\mathbf{Y}'\tilde{\mathbf{r}}} \\
&= g^{\mathbf{B}^{-1}\mathbf{Y}'(\mathbf{T}\mathbf{r})} \cdot g^{\mathbf{B}^{-1}\mathbf{Y}'(\gamma\tilde{\mathbf{r}})} \\
&= g^{\mathbf{B}^{-1}\mathbf{Y}'(\mathbf{T}\mathbf{r}+\gamma\tilde{\mathbf{r}})} \\
&= g^{\mathbf{B}^{-1}\mathbf{Y}'\mathbf{r}'}
\end{aligned}
\end{array}$$

The claim that delegation is independent of the path taken follows readily.

Proof of Security. It suffices to show how to compute MPK. On input selective challenge $(\mathbf{x}_0^*, \mathbf{X})$, we sample $(\bar{\mathbf{X}}, \mathbf{Z}, \bar{\mathbf{Z}}, \tilde{\mathbf{w}})$ as in Section 3.2, implicitly set

$$\mathbf{B}^\top \mathbf{X} = \mathbf{Z} \quad \text{and} \quad \mathbf{B}^\top \bar{\mathbf{X}} = a\bar{\mathbf{Z}} \quad \text{and} \quad \mathbf{w} := -\mathbf{B}^\top \mathbf{x}_0^* + \tilde{\mathbf{w}} \quad \text{and} \quad \alpha := ab,$$

and compute $(e(g,g)^\alpha, g^{\mathbf{w}}, g^{\mathbf{B}})$ as before. Next, we pick $\tilde{\gamma} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^*$ and implicitly set

$$\gamma := \tilde{\gamma} a.$$

We need to show how to compute the additional terms

$$g^{\gamma \mathbf{B}^{-1}} \quad \text{and} \quad g^{\gamma (\mathbf{B}^{-1})^\top \mathbf{w}}.$$

Recall that

$$\mathbf{B}^{-1} := a^{-1}((\mathbf{Z} \| \bar{\mathbf{Z}})^{-1})^\top (a\mathbf{X} \| \bar{\mathbf{X}})^\top,$$

thus

$$\gamma(\mathbf{B}^{-1})^\top := \tilde{\gamma}(a\mathbf{X} \| \bar{\mathbf{X}})(\mathbf{Z} \| \bar{\mathbf{Z}})^{-1}.$$

Then given g, g^a along with $\tilde{\gamma}, \mathbf{Z}, \bar{\mathbf{Z}}, \mathbf{X}, \bar{\mathbf{X}}$, we can compute $g^{\gamma(\mathbf{B}^{-1})^\top}$ (also obtain $g^{\gamma\mathbf{B}^{-1}}$ by matrix transpose) as

$$((g^a)^{\mathbf{X}} \| g^{\bar{\mathbf{X}}})^{\tilde{\gamma}(\mathbf{Z} \| \bar{\mathbf{Z}})^{-1}}$$

Also observe that

$$\gamma(\mathbf{B}^{-1})^\top \mathbf{w} = \gamma(\mathbf{B}^{-1})^\top(-\mathbf{B}^\top \mathbf{x}_0^* + \tilde{\mathbf{w}}) = -\tilde{\gamma} a \mathbf{x}_0^* + (\gamma \mathbf{B}^{-1})^\top \tilde{\mathbf{w}}$$

Here, we can compute $g^{\gamma(\mathbf{B}^{-1})^\top \mathbf{w}}$ as

$$(g^a)^{-\tilde{\gamma}\mathbf{x}_0^*} \cdot (g^{(\gamma\mathbf{B}^{-1})^\top})^{\tilde{\mathbf{w}}}.$$

References

[1] S. Agrawal, D. Boneh, and X. Boyen. Efficient lattice (H)IBE in the standard model. In *EUROCRYPT*, pages 553–572, 2010.

[2] S. Agrawal, D. M. Freeman, and V. Vaikuntanathan. Functional encryption for inner product predicates from learning with errors. In *ASIACRYPT*, pages 21–40, 2011.

[3] N. Attrapadung and B. Libert. Functional encryption for inner product: Achieving constant-size ciphertexts with adaptive security or support for negation. In *Public Key Cryptography*, pages 384–402, 2010.

[4] D. Boneh and X. Boyen. Efficient selective-id secure identity-based encryption without random oracles. In *EUROCRYPT*, pages 223–238, 2004.

[5] D. Boneh and M. K. Franklin. Identity-based encryption from the Weil pairing. *SIAM J. Comput.*, 32(3): 586–615, 2003.

[6] D. Boneh and M. Hamburg. Generalized identity based and broadcast encryption schemes. In *ASIACRYPT*, pages 455–470, 2008.

[7] D. Boneh, X. Boyen, and E.-J. Goh. Hierarchical identity based encryption with constant size ciphertext. In *EUROCRYPT*, pages 440–456, 2005.

[8] X. Boyen and L. Martin. Identity-based cryptography standard (IBCS) #1: Supersingular curve implementations of the BF and BB1 cryptosystems. IETF RFC 5091, Dec. 2007. URL http://www.rfc-editor.org/rfc/rfc5091.txt.

[9] X. Boyen and B. Waters. Anonymous hierarchical identity-based encryption (without random oracles). In *CRYPTO*, pages 290–307, 2006.

[10] R. Canetti, S. Halevi, and J. Katz. A forward-secure public-key encryption scheme. In *EUROCRYPT*, pages 255–271, 2003.

[11] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert. Bonsai trees, or how to delegate a lattice basis. In *EUROCRYPT*, pages 523–552, 2010.

[12] C. Chen, Z. Zhang, and D. Feng. Fully secure doubly-spatial encryption under simple assumptions. In *ProvSec*, pages 253–263, 2012.

[13] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *ACM Conference on Computer and Communications Security*, pages 89–98, 2006.

[14] M. Hamburg. Spatial encryption. *IACR Cryptology ePrint Archive*, 2011:389, 2011.

[15] J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In *EUROCRYPT*, pages 146–162, 2008.

[16] A. B. Lewko and B. Waters. New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In *TCC*, pages 455–479, 2010.

[17] 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 *EUROCRYPT*, pages 62–91, 2010.

[18] A. Sahai and B. Waters. Fuzzy identity-based encryption. In *EUROCRYPT*, pages 457–473, 2005.

[19] B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *Public Key Cryptography*, pages 53–70, 2011.

[20] M. Zhou and Z. Cao. Spatial encryption under simpler assumption. In *ProvSec*, pages 19–31, 2009.

A Generic Transformation for DSE

In this section, we show how to handle affine spaces for secret keys from a construction for linear spaces. It suffices to present an embedding similar to that in [6, Section 2.3] and [14, Section 2.5]. Specifically, starting with

$$(\mathbf{x}_0, \mathbf{X}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^{n\times d} \quad \text{and} \quad (\mathbf{y}_0, \mathbf{Y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^{n\times m},$$

we can compute

$$(\hat{\mathbf{x}}_0, \hat{\mathbf{X}}) \in \mathbb{Z}_p^{n+1} \times \mathbb{Z}_p^{(n+1)\times d} \quad \text{and} \quad \hat{\mathbf{Y}} \in \mathbb{Z}_p^{(n+1)\times(n-m)},$$

so that

$$(\mathbf{x}_0 + \mathrm{span}(\mathbf{X})) \cap (\mathbf{y}_0 + \mathrm{span}(\mathbf{Y})) \neq \emptyset \Leftrightarrow (\hat{\mathbf{x}}_0 + \mathrm{span}(\hat{\mathbf{X}})) \cap \ker(\hat{\mathbf{Y}}) \neq \emptyset.$$

Embedding. We embed an n-dimensional affine system into an $(n+1)$-dimensional linear system as follows:

- for any secret key associated with a vector matrix pair $(\mathbf{y}_0, \mathbf{Y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^{n\times m}$ specifying an affine space $\mathbf{y}_0 + \mathrm{span}(\mathbf{Y})$, we embed it into the *linear space* $\mathrm{span}(\tilde{\mathbf{Y}})$, where

$$\tilde{\mathbf{Y}} := \begin{pmatrix} 1 & \mathbf{0}^\top \\ \mathbf{y}_0 & \mathbf{Y} \end{pmatrix} \in \mathbb{Z}_p^{(n+1)\times(m+1)};$$

  Given $\tilde{\mathbf{Y}} \in \mathbb{Z}_p^{(n+1)\times(m+1)}$, we can easily compute $\hat{\mathbf{Y}} \in \mathbb{Z}_p^{(n+1)\times(n-m)}$ so that $\ker(\hat{\mathbf{Y}}) = \mathrm{span}(\tilde{\mathbf{Y}})$.
- for any ciphertext associated with a vector matrix pair $(\mathbf{x}_0, \mathbf{X}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^{n\times d}$ specifying an affine space $\mathbf{x}_0 + \mathrm{span}(\mathbf{X})$, we embed it into the *affine space* $\tilde{\mathbf{x}}_0 + \mathrm{span}(\tilde{\mathbf{X}})$, where

$$\tilde{\mathbf{x}}_0 := \begin{pmatrix} 1 \\ \mathbf{x}_0 \end{pmatrix} \in \mathbb{Z}_p^{(n+1)\times 1} \quad \text{and} \quad \tilde{\mathbf{X}} := \begin{pmatrix} \mathbf{0}^\top \\ \mathbf{X} \end{pmatrix} \in \mathbb{Z}_p^{(n+1)\times d}.$$

Correctness. Fix $(\mathbf{x}_0, \mathbf{X})$ and $(\mathbf{y}_0, \mathbf{Y})$ such that $(\mathbf{x}_0 + \mathrm{span}(\mathbf{X})) \cap (\mathbf{y}_0 + \mathrm{span}(\mathbf{Y})) \neq \emptyset$, observe that we have

$$\begin{aligned}
(\mathbf{x}_0 + \mathrm{span}(\mathbf{X})) \cap (\mathbf{y}_0 + \mathrm{span}(\mathbf{Y})) \neq \emptyset &\Leftrightarrow (\begin{pmatrix} 1 \\ \mathbf{x}_0 \end{pmatrix} + \mathrm{span}(\begin{pmatrix} \mathbf{0}^\top \\ \mathbf{X} \end{pmatrix})) \cap (\begin{pmatrix} 1 \\ \mathbf{y}_0 \end{pmatrix} + \mathrm{span}(\begin{pmatrix} \mathbf{0}^\top \\ \mathbf{Y} \end{pmatrix})) \neq \emptyset \\
&\Leftrightarrow (\begin{pmatrix} 1 \\ \mathbf{x}_0 \end{pmatrix} + \mathrm{span}(\begin{pmatrix} \mathbf{0}^\top \\ \mathbf{X} \end{pmatrix})) \cap \mathrm{span}(\begin{pmatrix} 1 & \mathbf{0}^\top \\ \mathbf{y}_0 & \mathbf{Y} \end{pmatrix}) \neq \emptyset \\
&\Leftrightarrow (\tilde{\mathbf{x}}_0 + \mathrm{span}(\tilde{\mathbf{X}})) \cap \mathrm{span}(\tilde{\mathbf{Y}}) \neq \emptyset.
\end{aligned}$$

Delegation. Fix $(\mathbf{y}_0, \mathbf{Y})$ and $(\mathbf{y}'_0, \mathbf{Y}')$ such that $(\mathbf{y}'_0 + \mathrm{span}(\mathbf{Y}')) \subseteq (\mathbf{y}_0 + \mathrm{span}(\mathbf{Y}))$, observe that we have

$$\begin{aligned}
(\mathbf{y}'_0 + \mathrm{span}(\mathbf{Y}')) \subseteq (\mathbf{y}_0 + \mathrm{span}(\mathbf{Y})) &\Leftrightarrow \mathbf{y}'_0 \in (\mathbf{y}_0 + \mathrm{span}(\mathbf{Y})) \wedge \mathrm{span}(\mathbf{Y}') \subseteq \mathrm{span}(\mathbf{Y}) \\
&\Leftrightarrow \begin{pmatrix} 1 \\ \mathbf{y}'_0 \end{pmatrix} \in \mathrm{span}(\begin{pmatrix} 1 & \mathbf{0}^\top \\ \mathbf{y}_0 & \mathbf{Y} \end{pmatrix}) \wedge \mathrm{span}(\begin{pmatrix} \mathbf{0}^\top \\ \mathbf{Y}' \end{pmatrix}) \subseteq \mathrm{span}(\begin{pmatrix} \mathbf{0}^\top \\ \mathbf{Y} \end{pmatrix}) \\
&\Leftrightarrow \mathrm{span}(\tilde{\mathbf{Y}}') \subseteq \mathrm{span}(\tilde{\mathbf{Y}}).
\end{aligned}$$

B NIPE from DSE

In this section, we show that NIPE can be naturally obtained from DSE defined in Section 2.1; our transformation is a special case of Hamburg's embedding of negated SE into DSE [14, Section 4.4]. In a NIPE scheme, both the ciphertext and the secret key are associated with vectors, a ciphertext $\textsc{ct}_{\mathbf{x}}$ can be decrypted by a secret key $\textsc{sk}_{\mathbf{y}}$ iff $\langle \mathbf{x}, \mathbf{y} \rangle \neq 0$.

Embedding. We embed an n-dimensional NIPE system into an $(n+1)$-dimensional DSE system as follows:

- for any secret key associated with a vector $\mathbf{y} \in \mathbb{Z}_p^n$, we embed it into the $(n+1)$-*dimensional vector* $\tilde{\mathbf{y}}$, where

$$\tilde{\mathbf{y}} := \begin{pmatrix} 1 \\ \mathbf{y} \end{pmatrix} \in \mathbb{Z}_p^{n+1}.$$

- for any ciphertext associated with a vector $\mathbf{x} \in \mathbb{Z}_p^n$, we embed it into the *affine space* $\tilde{\mathbf{1}}+\mathrm{span}(\tilde{\mathbf{x}})$, where

$$\tilde{\mathbf{1}} := \begin{pmatrix} 1 \\ \mathbf{0} \end{pmatrix} \in \mathbb{Z}_p^{n+1} \quad \text{and} \quad \tilde{\mathbf{x}} := \begin{pmatrix} 0 \\ \mathbf{x} \end{pmatrix} \in \mathbb{Z}_p^{n+1}.$$

Correctness. Fix $\mathbf{x}$ and $\mathbf{y}$ such that $\langle \mathbf{x}, \mathbf{y} \rangle \neq 0$, observe that we have

$$\begin{aligned} \langle \mathbf{x}, \mathbf{y} \rangle \neq 0 &\Leftrightarrow 1 - \langle \frac{1}{\langle \mathbf{x}, \mathbf{y} \rangle} \mathbf{x}, \mathbf{y} \rangle = 0 \\ &\Leftrightarrow \langle \begin{pmatrix} 1 \\ \mathbf{0} \end{pmatrix} - \frac{1}{\langle \mathbf{x}, \mathbf{y} \rangle} \begin{pmatrix} 0 \\ \mathbf{x} \end{pmatrix}, \begin{pmatrix} 1 \\ \mathbf{y} \end{pmatrix} \rangle = 0 \\ &\Leftrightarrow (\tilde{\mathbf{1}} + \mathrm{span}(\tilde{\mathbf{x}})) \cap \ker(\tilde{\mathbf{y}}) \neq \emptyset. \end{aligned}$$

Note that if $\langle \mathbf{x}, \mathbf{y} \rangle = 0$, we have $(\tilde{\mathbf{1}} + \mathrm{span}(\tilde{\mathbf{x}})) \cap \ker(\tilde{\mathbf{y}}) = \emptyset$ since

$$\langle \tilde{\mathbf{1}} + u\tilde{\mathbf{x}}, \tilde{\mathbf{y}} \rangle = 1 + u\langle \mathbf{x}, \mathbf{y} \rangle = 1 \quad \forall u \in \mathbb{Z}_p.$$

C Self-Contained NIPE

In this section, we give a self-contained description of our NIPE scheme. Combined with our DSE scheme in Section 3.1 and generic transformation in Appendix B, we obtain an n-dimensional NIPE scheme based on DBDH with the following parameters:

$$|\text{MPK}| = (n^2 + 3n + 3)|G| + |G_T| \quad \text{and} \quad |\text{SK}| = (n+2)|G| \quad \text{and} \quad |\text{CT}| = (2n+3)|G| + |G_T|.$$

- $\mathsf{Setup}(1^\lambda, 1^{n+1})$: On input $(1^\lambda, 1^{n+1})$, generate $\mathbb{G} := (p, G, G_T, e) \leftarrow_{\mathrm{R}} \mathcal{G}(1^\lambda)$, pick $\alpha \leftarrow_{\mathrm{R}} \mathbb{Z}_p$, $\mathbf{w} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{n+1}$, $[\mathbf{b}_0 \| \mathbf{B}_1] \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{(n+1)\times(n+1)}$, and output

$$\text{MPK} := \Big(\ \mathbb{G}; e(g,g)^\alpha, g, g^{\mathbf{w}}, g^{\mathbf{b}_0}, g^{\mathbf{B}_1}\ \Big) \in G_T \times G \times G^{n+1} \times G^{n+1} \times G^{n\times(n+1)}$$

  and

$$\text{MSK} := (\ \alpha, \mathbf{w}, \mathbf{b}_0^*, \mathbf{B}_1^*\ ) \in \mathbb{Z}_p \times \mathbb{Z}_p^{n+1} \times \mathbb{Z}_p^{n+1} \times \mathbb{Z}_p^{n\times(n+1)},$$

  where $[\mathbf{b}_0 \| \mathbf{B}_1]^{-1} = [\mathbf{b}_0^* \| \mathbf{B}_1^*]^\top$.
- $\mathsf{Enc}(\text{MPK}, \mathbf{x}, m)$: On input $\mathbf{x} \in \mathbb{Z}_p^n$, and message $m \in G_T$, pick $s \leftarrow_{\mathrm{R}} \mathbb{Z}_p$ and output

$$\begin{aligned} \text{CT}_{\mathbf{x}} := \Big(\ C_0 := g^s,\ \mathbf{C}_1 := g^{(\mathbf{b}_0+\mathbf{w})s},\ \mathbf{C}_2 := g^{\mathbf{B}_1\mathbf{x}s},\ C' := e(g,g)^{\alpha s}\cdot m\ \Big) \\ \in G \times G^{n+1} \times G^{n+1} \times G_T. \end{aligned}$$

- $\mathsf{KeyGen}(\text{MPK}, \text{MSK}, \mathbf{y})$: On input $\mathbf{y} \in \mathbb{Z}_p^n$, pick $r \leftarrow_{\text{R}} \mathbb{Z}_p$ and output

$$\text{SK}_{\mathbf{y}} := \Big(\ K_0 := g^{\alpha - r\langle \mathbf{w}, \mathbf{b}_0^* + \mathbf{B}_1^* \mathbf{y}\rangle},\ \mathbf{K}_1 := g^{r(\mathbf{b}_0^* + \mathbf{B}_1^* \mathbf{y})}\ \Big) \in G \times G^{n+1}.$$

- $\mathsf{Dec}(\text{MPK}, \text{SK}_{\mathbf{y}}, \text{CT}_{\mathbf{x}})$: If $\langle \mathbf{x}, \mathbf{y}\rangle \neq 0$, parse the ciphertext as $(C_0, \mathbf{C}_1, \mathbf{C}_2, C')$ and compute

$$e(g,g)^{\alpha s} \leftarrow e(C_0, K_0) \cdot e(\mathbf{C}_1 \cdot \mathbf{C}_2^{-\frac{1}{\langle \mathbf{x}, \mathbf{y}\rangle}}, \mathbf{K}_1).$$

  Recover the message as $m \leftarrow C'/e(g,g)^{\alpha s} \in G_T$.

Correctness. Fix $\mathbf{x}$ and $\mathbf{y}$ such that $\langle \mathbf{x}, \mathbf{y}\rangle \neq 0$, correctness follows readily from Section 3.1 since we have

$$\langle \begin{pmatrix} 1 \\ \mathbf{0} \end{pmatrix} - \frac{1}{\langle \mathbf{x}, \mathbf{y}\rangle} \begin{pmatrix} 0 \\ \mathbf{x} \end{pmatrix}, \begin{pmatrix} 1 \\ \mathbf{y} \end{pmatrix} \rangle = 0$$