Shorter IBE and Signatures via Asymmetric Pairings

Jie Chen[1], Hoon Wei Lim[1], San Ling[1], Huaxiong Wang[1], and Hoeteck Wee[2,1⋆]

[1] Division of Mathematical Sciences
School of Physical & Mathematical Sciences
Nanyang Technological University, Singapore
[2] Department of Computer Science
George Washington University, USA
s080001@e.ntu.edu.sg
{hoonwei,lingsan,hxwang}@ntu.edu.sg
hoeteck@gwu.edu

Abstract. We present efficient Identity-Based Encryption (IBE) and signature schemes under the Symmetric External Diffie-Hellman (SXDH) assumption in bilinear groups. In both the IBE and the signature schemes, all parameters have constant numbers of group elements, and are shorter than those of previous constructions based on Decisional Linear (DLIN) assumption. Our constructions use both dual system encryption (Waters, Crypto '09) and dual pairing vector spaces (Okamoto and Takashima, Pairing '08, Asiacrypt '09). Specifically, we show how to adapt the recent DLIN-based instantiations of Lewko (Eurocrypt '12) to the SXDH assumption. To our knowledge, this is the first work to instantiate either dual system encryption or dual pairing vector spaces under the SXDH assumption.

⋆ Research of the authors is supported in part by the National Research Foundation of Singapore under Research Grant NRF-CRP2-2007-03. Hoeteck Wee's work is also supported by NSF CAREER Award CNS-1237429.

1 Introduction

Identity-Based Encryption. The idea of using a user's identity as her public encryption key, and thus eliminating the need for a public key certificate, was conceived by Shamir [33]. Such a primitive is known as Identity-Based Encryption (IBE), which has been extensively studied particularly over the last decade. We now have constructions of IBE schemes from a large class of assumptions, namely pairings, quadratic residuosity and lattices, starting with the early constructions in the random oracle model [9, 16, 22], to more recent constructions in the standard model [14, 7, 8, 15, 2].

Short IBE. It is desirable that an IBE scheme be as efficient as possible, if it were to have any impact on practical applications. Ideally, we would like to have constant-size public parameters, secret keys, and ciphertexts. Moreover, the scheme should ideally achieve full security, namely to be resilient even against an adversary that adaptively selects an identity to attack based on previous secret keys. The first fully secure efficient IBE with constant-size public parameters and ciphertexts under standard assumptions was obtained by Waters [36] in 2009; this scheme relied on the Decisional Bilinear Diffie-Hellman (DBDH) and Decisional Linear (DLIN) assumptions. Since then, Lewko and Waters [26] and Lewko [25] gave additional fully secure efficient IBE schemes that achieve incomparable guarantees. Prior to these works, all known IBEs (in the standard model) were either selectively secure [14, 7, 15, 2], or require long parameters [8, 35, 15, 2], or were based on less standard assumptions that depended on the query complexity of the adversary [21]. From a practical stand-point, Waters' fully secure IBE [36] is still not very efficient as it has relatively large ciphertexts and secret keys, i.e., eleven and nine group elements,[1] respectively. Lewko's scheme [25] improved on both of these parameters at the cost of larger public parameters and master key.

Shorter IBE? In his work, Waters also suggested obtaining even more efficient IBE schemes by turning to asymmetric bilinear groups:

> Using the SXDH assumption we might hope to shave off three group elements from both ciphertexts and private keys.

In fact, improving the efficiency of a scheme using asymmetric pairings was first observed by Boneh, Boyen and Shacham [10]. At a fixed security level, group elements in the asymmetric setting are smaller and pairings can be computed more efficiently [19]. (Estimated bit sizes of group elements for bilinear group generators are given in Appendix A.) Informally, the SXDH assumption states that there are prime-order groups (G_1, G_2, G_T) that admits a bilinear map $e : G_1 \times G_2 \to G_T$ such that the Decisional Diffie-Hellman (DDH) assumption holds in both G_1 and G_2. The SXDH assumption was formally defined by Ballard et al. [4] in their construction of a searchable encryption scheme, and has since been used in a number of different contexts, including secret-handshake schemes [3], anonymous IBE [17], continual leakage-resilience [12], and most notably, Groth-Sahai proofs [24]. Evidence for the validity of this assumption were presented in the works of Verheul [34] and Galbraith and Rotger [20].

[1] Here, we do not separately consider group elements from target groups of pairings, although a ciphertext typically has a group element that is from an associated target group.

1.1 Our Contributions

In this work, we present a more efficient IBE scheme under the SXDH assumption; our scheme also achieves anonymity.[2] The ciphertexts and secret keys consist of only five and four group elements, respectively. That is, we shave off two group elements from both ciphertexts and private keys in Lewko's DLIN-based IBE [25]. See Table 1 for a summary of comparisons between existing and our IBE schemes, where λ is the security parameter. Applying Naor's transform [9, 11] to our scheme, we also obtain an efficient signature scheme.

Source	# PP	# MK	# SK	# CT	# pairing	anonymity	assumptions
Waters [35]	$\mathcal{O}(\lambda)$	1	2	3	2	No	DBDH
Waters [36]	13	5	9	11	9	No	DLIN,DBDH
Lewko [25]	25	30	6	7	6	Yes	DLIN
RCS [32]	9	7	7	9	7	No	XDH, DLIN, DBDH
Ours	9	9	4	5	4	Yes	SXDH

Table 1. Comparison between existing and our IBE schemes.

Our approach. As with all known fully secure efficient IBEs, our construction relies on Waters' dual system encryption framework [36]. Following Lewko's DLIN-based IBE [25], we instantiate dual system encryption under the SXDH assumption via dual pairing vector spaces [29, 30], which is a technique to achieve orthogonality in prime-order groups. This is the first work to instantiate either dual system encryption or dual pairing vector spaces under the SXDH assumption. We proceed to highlight several salient features of our IBE scheme in relation to Lewko's IBE [25]:

- Our scheme has an extremely simple structure, similar to the selectively secure IBE of Boneh and Boyen [7], as well as the fully secure analogues given by Lewko and Waters [26] and Lewko [25].
- By shifting from the DLIN assumption to the simpler SXDH assumption, we obtain IBE schemes that are syntactically simpler and achieve shorter parameters. Specifically, Lewko's IBE scheme [25] relies on 6 basis vectors to simulate the subgroup structure in the Lewko-Waters IBE scheme [26], whereas our construction uses only 4 basis vectors. This means that we can use a 4-dimensional vector space instead of a 6-dimensional one. As a result, we save two group elements in both the secret key and the ciphertext, that is, by a factor of 1/3. The savings for the public parameters and master key is even more substantial, because we use only two basis vectors for the main scheme, as opposed to four basis vectors in Lewko's scheme. In both our scheme and in Lewko's, the remaining two basis vectors are used for the semi-functional components in the proof of security.
- The final step of the proof of security (after switching to semi-functional secret keys and ciphertexts) is different from that of Lewko's. We rely on an information theoretic argument similar to that in [31] instead of computational arguments.

Finally, we believe that our SXDH instantiations constitute a simpler demonstration of the power of dual pairing vector spaces.

[2] It follows from our analysis that Lewko's IBE [25] is also anonymous, although this was not pointed out in her paper.

Independent work of Ramanna et al. An independent work of Ramanna, Chatterjee and Sarkar [32] also demonstrated how to obtain more efficient fully secure IBE via asymmetric pairings. Similar to our work, their constructions rely on dual system encryption; however, they do not make use of dual pairing vector spaces. Our constructions achieve shorter ciphertexts and secret keys than their work, while relying on a single assumption (whereas their construction relies on a triplet of assumptions). Moreover, our scheme achieves anonymity; theirs does not. Finally, they obtain their schemes via careful optimizations, whereas our scheme is derived via a more general framework.

Outline. In Section 2, we present the preliminaries, including security definitions for IBE, our security assumptions, and an overview of dual pairing vector spaces. In Section 3, we present the subspace assumptions based on SXDH. Finally, we present our IBE and signature schemes in Sections 4 and 5.

2 Preliminaries

In this section, we first recall the definitions of security for IBE, and signatures. We then present a few backgrounds related to groups with efficiently computable bilinear maps and define the Symmetric External Diffie-Hellman assumption.

2.1 Identity-Based Encryption and Signatures

Identity-Based Encryption. An Identity-Based Encryption [9] scheme consists of four algorithms: $(\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$:

- $\mathsf{Setup}(\lambda) \to \mathsf{PP}, \mathsf{MK}$ The setup algorithm takes in the security parameter λ, and outputs the public parameters PP, and the master key MK.
- $\mathsf{KeyGen}(\mathsf{PP}, \mathsf{MK}, ID) \to \mathsf{SK}_{ID}$ The key generation algorithm takes in the master key MK, and an identity ID, and produces a secret key SK_{ID} for that identity.
- $\mathsf{Enc}(\mathsf{PP}, ID, M) \to \mathsf{CT}_{ID}$ The encryption algorithm takes in an identity ID, and a message M, and outputs a ciphertext CT_{ID} encrypted under that identity.
- $\mathsf{Dec}(\mathsf{PP}, \mathsf{SK}_{ID}, \mathsf{CT}_{ID}) \to M$ The decryption algorithm takes in a secret key SK_{ID}, and a ciphertext CT_{ID}, and outputs the message M when the CT_{ID} is encrypted under the same ID.

Anonymous IBE. The security notion of anonymous IBE was formalized by [1], which is defined by the following game, played by a challenger $\mathcal{B}$ and an adversary $\mathcal{A}$.

- Setup The challenger $\mathcal{B}$ runs the setup algorithm to generate PP and MK. It gives PP to the adversary $\mathcal{A}$.
- $\mathsf{Phase\ 1}$ The challenger $\mathcal{A}$ adaptively requests keys for identities ID, and is provided with corresponding secret keys SK_{ID}, which the challenger $\mathcal{B}$ generates by running the key generation algorithm.
- $\mathsf{Challenge}$ The adversary $\mathcal{A}$ gives the challenger $\mathcal{B}$ two challenge pairs (M_0, ID_0^*) and (M_1, ID_1^*). The challenge identities must not have been queried in Phase 1. The challenger sets $\beta \in \{0, 1\}$ randomly, and encrypts M_β under ID_β^* by running the encryption algorithm. It sends the ciphertext to the adversary $\mathcal{A}$.
- $\mathsf{Phase\ 2}$ This is the same as Phase 1, with the added restriction a secret key for ID_0^*, ID_1^* cannot be requested.

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

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

Definition 1. *An Identity-Based Encryption scheme is secure and anonymous if all PPT adversaries achieve at most a negligible advantage in the above security game.*

Remark: The security notion of non-anonymous IBE is defined as above with restriction that $ID^*_0 = ID^*_1$.

Signatures. A signature scheme is made up of three algorithms, $(\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$ for generating keys, signing, and verifying signatures, respectively.

– $\mathsf{KeyGen}(1^\lambda) \to \mathsf{PK}, \mathsf{SK}$ The key generation algorithm takes in the security parameter λ, and outputs the public key PK, and the secret key SK.
– $\mathsf{Sign}(\mathsf{SK}, M) \to \sigma$ The signing algorithm takes in the secret key SK, and a message M, and produces a signature σ for that message.
– $\mathsf{Verify}(\mathsf{PK}, \sigma, M) \to \mathsf{CT}$ The verifying algorithm takes in the public key PK, and a signature pair (σ, M), and outputs `valid` or `invalid`.

The standard notion of security for a signature scheme is called existential unforgeability under a chosen message attack [23], which is defined using the following game between a challenger $\mathcal{B}$ and an adversary $\mathcal{A}$.

– Setup The challenger $\mathcal{B}$ runs the setup algorithm to generate PK and SK. It gives PK to the adversary $\mathcal{A}$.
– $\mathsf{Queries}$ The adversary $\mathcal{A}$ adaptively requests for messages $M_1, \ldots, M_\nu \in \{0,1\}^*$, and is provided with corresponding signatures $\sigma_1, \ldots, \sigma_\nu$ by running the sign algorithm Sign.
– Output Eventually, the adversary $\mathcal{A}$ outputs a pair (M, σ).

The advantage $\mathsf{Adv}^{\mathsf{Sig}}_{\mathcal{A}}(\lambda)$ of an adversary $\mathcal{A}$ is defined to be the probability that $\mathcal{A}$ wins in the above game, namely

(1) M is not any of $M_1, \ldots, M_\nu$;
(2) $\mathsf{Verify}(\mathsf{PK}, \sigma, M)$ outputs `valid`.

Definition 2. *A signature scheme is existentially unforgeable under an adaptive chosen message attack if all PPT adversaries achieve at most a negligible advantage in the above security game.*

We assume that for any PPT algorithm $\mathcal{A}$, the probability that $\mathcal{A}$ wins in the above game is negligible in the security parameter λ.

2.2 Dual Pairing Vector Spaces

Our constructions are based on dual pairing vector spaces proposed by Okamoto and Takashima [29, 30]. In this paper, we concentrate on the asymmetric version [31]. We only briefly describe how to generate random dual orthonormal bases. See [29, 30, 31] for a full definition of dual pairing vector spaces.

Definition 3. *"Asymmetric bilinear pairing groups"* $(q, G_1, G_2, G_T, g_1, g_2, e)$ *are a tuple of a prime* q*, cyclic (multiplicative) groups* G_1, G_2 *and* G_T *of order* q*,* $g_1 \neq 1 \in G_1$*,* $g_2 \neq 1 \in G_2$*, and a polynomial-time computable nondegenerate bilinear pairing* $e : G_1 \times G_2 \to G_T$ *i.e.,* $e(g_1^s, g_2^t) = e(g_1, g_2)^{st}$ *and* $e(g_1, g_2) \neq 1$*.*

In addition to referring to individual elements of G_1 or G_2, we will also consider "vectors" of group elements. For $\boldsymbol{v} = (v_1, \ldots, v_n) \in \mathbb{Z}_q^n$ and $g_\beta \in G_\beta$, we write $g_\beta^{\boldsymbol{v}}$ to denote a n-tuple of elements of G_β for $\beta = 1, 2$:

$$g_\beta^{\boldsymbol{v}} := (g_\beta^{v_1}, \ldots, g_\beta^{v_n}).$$

For any $a \in \mathbb{Z}_q$ and $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{Z}_q^n$, we have:

$$g_\beta^{a\boldsymbol{v}} := (g_\beta^{av_1}, \ldots, g_\beta^{av_n}), \quad g_\beta^{\boldsymbol{v}+\boldsymbol{w}} := (g_\beta^{v_1+w_1}, \ldots, g_\beta^{v_n+w_n}).$$

Then we define

$$e(g_1^{\boldsymbol{v}}, g_2^{\boldsymbol{w}}) := \prod_{i=1}^{n} e(g_1^{v_i}, g_2^{w_i}) = e(g_1, g_2)^{\boldsymbol{v}\cdot\boldsymbol{w}}.$$

Here, the dot product is taken modulo q.

Dual Pairing Vector Spaces. For a fixed (constant) dimension n, we will choose two random bases $\mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ and $\mathbb{B}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_n^*)$ of $\mathbb{Z}_q^n$, subject to the constraint that they are "dual orthonormal", meaning that

$$\boldsymbol{b}_i \cdot \boldsymbol{b}_j^* = 0 \,(\mathrm{mod}\ q)$$

whenever $i \neq j$, and

$$\boldsymbol{b}_i \cdot \boldsymbol{b}_i^* = \psi \,(\mathrm{mod}\ q)$$

for all i, where ψ is a random element of $\mathbb{Z}_q$. We denote such algorithm as $\mathsf{Dual}(\cdot)$.

Then for generators $g_1 \in G_1$ and $g_2 \in G_2$, we have

$$e(g_1^{\boldsymbol{b}_i}, g_2^{\boldsymbol{b}_j^*}) = 1$$

whenever $i \neq j$, where 1 here denotes the identity element in G_T.

2.3 SXDH Assumptions

Definition 4. *[DDH1: Decisional Diffie-Hellman Assumption in* G_1*] Given a group generator* $\mathcal{G}$*, we define the following distribution:*

$$\begin{aligned}
&\mathbb{G} := (q, G_1, G_2, G_T, g_1, g_2, e) \xleftarrow{R} \mathcal{G},\\
&a, b, c \xleftarrow{R} \mathbb{Z}_q,\\
&D := (\mathbb{G}; g_1, g_2, g_1^a, g_1^b).
\end{aligned}$$

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

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DDH1}}(\lambda) := \left| \Pr[\mathcal{A}(D, g_1^{ab}) - \Pr[\mathcal{A}(D, g_1^{ab+c})] \right|.$$

is negligible in the security parameter λ*.*

The dual of above assumption is Decisional Diffie-Hellman assumption in G_2 (denoted as DDH2), which is identical to Definitions 4 with the roles of G_1 and G_2 reversed. We say that:

Definition 5. *The Symmetric External Diffie-Hellman assumption holds if DDH problems are intractable in both G_1 and G_2.*

2.4 Statistical Indistinguishability Lemma

We require the following lemma from [27] in our security proof.

Lemma 1. *Let $C := \{(\boldsymbol{x}, \boldsymbol{v}) | \boldsymbol{x} \cdot \boldsymbol{v} \neq 0, \boldsymbol{x}, \boldsymbol{v} \in \mathbb{Z}_q^n\}$. For all $(\boldsymbol{x}, \boldsymbol{v}) \in C$, $(\boldsymbol{r}, \boldsymbol{w}) \in C$, $\rho, \tau \leftarrow \mathbb{Z}_q$, and $A \xleftarrow{R} \mathbb{Z}_q^{n \times n}$,*

$$\Pr[\boldsymbol{x}(\rho A^{-1}) = \boldsymbol{r} \wedge \boldsymbol{v}(\tau A^t) = \boldsymbol{w}] = \frac{1}{\#C},$$

where $\#C = (q^n - 1)(q^n - q^{n-1})$.

In other words, $(\rho \boldsymbol{x} A^{-1})$ and $(\tau \boldsymbol{v} A^t)$ are uniformly and independently distributed (i.e., equivalently distributed to $(\boldsymbol{r}, \boldsymbol{w}) \xleftarrow{R} \mathbb{Z}_q^n \times \mathbb{Z}_q^n$ where $\boldsymbol{r} \cdot \boldsymbol{w} \neq 0$, while $\Pr[\boldsymbol{r} \cdot \boldsymbol{w} = 0] = 1/q$) when $\boldsymbol{x} \cdot \boldsymbol{v} \neq 0$.

3 Subspace Assumptions via SXDH

In this section, we present Subspace assumptions derived from the SXDH assumption. We will rely on these assumptions later to instantiate our IBE scheme. These are analogues of the DLIN-based Subspace assumptions given in [25, 31].

Definition 6. *[DS1: Decisional Subspace Assumption in G_1] Given a group generator $\mathcal{G}(\cdot)$, define the following distribution:*

$$\begin{aligned}
&\mathbb{G} := (q, G_1, G_2, G_T, g_1, g_2, e) \xleftarrow{R} \mathcal{G}(1^\lambda),\\
&(\mathbb{B}, \mathbb{B}^*) \xleftarrow{R} \mathsf{Dual}(\mathbb{Z}_q^n),\\
&\tau_1, \tau_2, \mu_1, \mu_2 \xleftarrow{R} \mathbb{Z}_q,\\
&U_1 := g_2^{\mu_1 \boldsymbol{b}_1^* + \mu_2 \boldsymbol{b}_{k+1}^*}, U_2 := g_2^{\mu_1 \boldsymbol{b}_2^* + \mu_2 \boldsymbol{b}_{k+2}^*}, \ldots, \ldots, U_k := g_2^{\mu_1 \boldsymbol{b}_k^* + \mu_2 \boldsymbol{b}_{2k}^*},\\
&V_1 := g_1^{\tau_1 \boldsymbol{b}_1}, V_2 := g_1^{\tau_1 \boldsymbol{b}_2}, \ldots, V_k := g_1^{\tau_1 \boldsymbol{b}_k},\\
&W_1 := g_1^{\tau_1 \boldsymbol{b}_1 + \tau_2 \boldsymbol{b}_{k+1}}, W_2 := g_1^{\tau_1 \boldsymbol{b}_2 + \tau_2 \boldsymbol{b}_{k+2}}, \ldots, W_k := g_1^{\tau_1 \boldsymbol{b}_k + \tau_2 \boldsymbol{b}_{2k}},\\
D := (\mathbb{G}; &g_2^{\boldsymbol{b}_1^*}, g_2^{\boldsymbol{b}_2^*}, \ldots, g_2^{\boldsymbol{b}_k^*}, g_2^{\boldsymbol{b}_{2k+1}^*}, \ldots, g_2^{\boldsymbol{b}_n^*}, g_1^{\boldsymbol{b}_1}, \ldots, g_1^{\boldsymbol{b}_n}, U_1, U_2, \ldots, U_k, \mu_2),
\end{aligned}$$

where k, n are fixed positive integers that satisfy $2k \leq n$. We assume that for any PPT algorithm $\mathcal{A}$ (with output in $\{0, 1\}$),

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DS1}}(\lambda) := |\Pr[\mathcal{A}(D, V_1, \ldots, V_k) = 1] - \Pr[\mathcal{A}(D, W_1, \ldots, W_k) = 1]|$$

is negligible in the security parameter λ.

For our construction, we only require the assumption for $n = 4, k = 2$. Furthermore, we do not need to provide μ_2 to the distinguisher. Informally, this means that, given:

$$\tau_1, \tau_2, \mu_1, \mu_2 \xleftarrow{R} \mathbb{Z}_q; \qquad \text{and} \qquad U_1 := g_2^{\mu_1 \boldsymbol{b}_1^* + \mu_2 \boldsymbol{b}_3^*}, U_2 := g_2^{\mu_1 \boldsymbol{b}_2^* + \mu_2 \boldsymbol{b}_4^*},$$

the distributions (V_1, V_2) and (W_1, W_2) are computationally indistinguishable, where:

$$V_1 := g_1^{\tau_1 \boldsymbol{b}_1}, V_2 := g_1^{\tau_1 \boldsymbol{b}_2},$$
$$W_1 := g_1^{\tau_1 \boldsymbol{b}_1 + \tau_2 \boldsymbol{b}_3}, W_2 := g_1^{\tau_1 \boldsymbol{b}_2 + \tau_2 \boldsymbol{b}_4}.$$

Lemma 2. *If the DDH assumption in G_1 holds, then the Subspace assumption in G_1 stated in Definition 6 also holds. More precisely, for any adversary $\mathcal{A}$ against the Subspace assumption in G_1, there exist probabilistic algorithms $\mathcal{B}$ whose running times are essentially the same as that of $\mathcal{A}$, such that*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DS1}}(\lambda) \leq \mathsf{Adv}_{\mathcal{B}}^{\mathsf{DDH1}}(\lambda).$$

Proof. We assume there exists a PPT algorithm $\mathcal{A}$ breaking the Subspace assumption with non-negligible advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DS1}}(\lambda)$ (for some fixed positive integers k, n satisfying $n \geq 2k$). We create a PPT algorithm $\mathcal{B}$ which breaks the DDH assumption in G_1 with non-negligible advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DS1}}(\lambda)$. $\mathcal{B}$ is given $g_1, g_2, g_1^a, g_1^b, T$, where T is either g_1^{ab} or T is a uniformly random element of G_1.

$\mathcal{B}$ first samples random dual orthonormal bases, denoted by $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_n$ and $\boldsymbol{f}_1^*, \ldots, \boldsymbol{f}_n^*$. From the definition, $\mathcal{B}$ chooses vectors $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_n, \boldsymbol{f}_1^*, \ldots, \boldsymbol{f}_n^*$ randomly, subject to the constraints that $\boldsymbol{f}_i \cdot \boldsymbol{f}_j^* \equiv 0 \pmod q$ when $i \neq j$, and $\boldsymbol{f}_i \cdot \boldsymbol{f}_i^* \equiv \psi \pmod q$ for all i from 1 to n, where ψ is a random element of $\mathbb{Z}_q$. Then, $\mathcal{B}$ implicitly sets:

$$\boldsymbol{b}_1 := \boldsymbol{f}_1 + a\boldsymbol{f}_{k+1}, \boldsymbol{b}_2 := \boldsymbol{f}_2 + a\boldsymbol{f}_{k+2}, \ldots, \boldsymbol{b}_k := \boldsymbol{f}_k + a\boldsymbol{f}_{2k},$$
$$\boldsymbol{b}_{k+1} := \boldsymbol{f}_{k+1}, \ldots, \boldsymbol{b}_n := \boldsymbol{f}_n.$$

$\mathcal{B}$ also sets the dual basis as:

$$\boldsymbol{b}_1^* := \boldsymbol{f}_1^*, \boldsymbol{b}_2^* := \boldsymbol{f}_2^*, \ldots, \boldsymbol{b}_k^* := \boldsymbol{f}_k^*,$$
$$\boldsymbol{b}_{k+1}^* := \boldsymbol{f}_{k+1}^* - a\boldsymbol{f}_1^*, \ldots, \boldsymbol{b}_{2k}^* := \boldsymbol{f}_{2k}^* - a\boldsymbol{f}_k^*,$$
$$\boldsymbol{b}_{2k+1}^* := \boldsymbol{f}_{2k+1}^*, \ldots, \boldsymbol{b}_n^* := \boldsymbol{f}_n^*.$$

We observe that under these definitions, $\boldsymbol{b}_i \cdot \boldsymbol{b}_j^* \equiv 0 \pmod q$ when $i \neq j$, and $\boldsymbol{b}_i \cdot \boldsymbol{b}_i^* \equiv \psi \pmod q$ for all i from 1 to n. We note that $\mathcal{B}$ can produce all of $g_1^{\boldsymbol{b}_1}, \ldots, g_1^{\boldsymbol{b}_n}$ (given g_1, g_1^a) as well as $g_2^{\boldsymbol{b}_1^*}, \ldots, g_2^{\boldsymbol{b}_k^*}$ and $g_2^{\boldsymbol{b}_{2k+1}^*}, \ldots, g_2^{\boldsymbol{b}_n^*}$ (given g_2). However, $\mathcal{B}$ cannot produce $g_2^{\boldsymbol{b}_{k+1}^*}, \ldots, g_2^{\boldsymbol{b}_{2k}^*}$ (these require knowledge of g_2^a). It is not difficult to check that $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ and $\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_n^*$ are properly distributed.

Now $\mathcal{B}$ creates $U_1, \ldots, U_k$ by choosing random values $\mu_1', \mu_2' \in \mathbb{Z}_q$ and setting:

$$U_1 := g_2^{\mu_1' \boldsymbol{b}_1^* + \mu_2' \boldsymbol{f}_{k+1}^*} := g_2^{(\mu_1' + a\mu_2') \boldsymbol{b}_1^* + \mu_2' \boldsymbol{b}_{k+1}^*}.$$

In other words, $\mathcal{B}$ has implicitly set $\mu_1 := \mu_1' + a\mu_2'$ and $\mu_2 := \mu_2'$. We note that these values are uniformly random, and μ_2 is known to $\mathcal{B}$. $\mathcal{B}$ can then form $U_2, \ldots, U_k$ as:

$$U_2 := g_2^{\mu_1' \boldsymbol{b}_2^* + \mu_2' \boldsymbol{f}_{k+2}^*}, \ldots, U_k := g_2^{\mu_1' \boldsymbol{b}_k^* + \mu_2' \boldsymbol{f}_{2k}^*}.$$

$\mathcal{B}$ implicitly sets $\tau_1 := b, \tau_2 := c$ and computes:

$$T_1 := T^{\boldsymbol{f}_{k+1}} \cdot (g_1^b)^{\boldsymbol{f}_1}, \ldots, T_k := T^{\boldsymbol{f}_{2k}} \cdot (g_1^b)^{\boldsymbol{f}_k}.$$

If $T = g_1^{ab}$, then these are distributed as $V_1, \ldots, V_k$, since

$$T^{\boldsymbol{f}_{k+i}} \cdot (g_1^b)^{\boldsymbol{f}_i} = g_1^{\tau_1 \boldsymbol{b}_i}.$$

If $T = g_1^{ab+c}$, then these are distributed as $W_1, \ldots, W_k$, since

$$T^{\boldsymbol{f}_{k+i}} \cdot (g_1^b)^{\boldsymbol{f}_i} = g_1^{\tau_1 \boldsymbol{b}_i + \tau_2 \boldsymbol{b}_{k+i}}.$$

$\mathcal{B}$ then gives

$$D := (\mathbb{G}; g_2^{\boldsymbol{b}_1^*}, g_2^{\boldsymbol{b}_2^*}, \ldots, g_2^{\boldsymbol{b}_k^*}, g_2^{\boldsymbol{b}_{2k+1}^*}, \ldots, g_2^{\boldsymbol{b}_n^*}, g_1^{\boldsymbol{b}_1}, \ldots, g_1^{\boldsymbol{b}_n}, U_1, U_2, \ldots, U_k, \mu_2)$$

to $\mathcal{A}$, along with $T_1, \ldots, T_k$. $\mathcal{B}$ can then leverage $\mathcal{A}$'s advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DS1}}(\lambda)$ in distinguishing between the distributions $(V_1, \ldots, V_k)$ and $(W_1, \ldots, W_k)$ to achieve an advantage $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{DDH1}}(\lambda)$ in distinguishing $T = g_1^{ab}$ from $T = g_1^{ab+c}$, hence violating the DDH assumption in G_1.

The dual of the Subspace assumption in G_1 is Subspace assumption in G_2 (denoted as DS2), which is identical to Definitions 6 with the roles of G_1 and G_2 reversed. Similarly, we can prove that the Subspace assumption holds in G_2 if the DDH assumption in G_2 holds.

4 Identity-Based Encryption

We now present our IBE construction along with our proof of its security under the SXDH assumption.

Construction. We begin with our IBE scheme:

- $\mathsf{Setup}(1^\lambda)$ This algorithm takes in the security parameter λ and generates a bilinear pairing $\mathbb{G} := (q, G_1, G_2, G_T, g_1, g_2, e)$ for sufficiently large prime order q. The algorithm samples random dual orthonormal bases, $(\mathbb{D}, \mathbb{D}^*) \xleftarrow{R} \mathsf{Dual}(\mathbb{Z}_q^4)$. Let $\boldsymbol{d}_1, \ldots, \boldsymbol{d}_4$ denote the elements of $\mathbb{D}$ and $\boldsymbol{d}_1^*, \ldots, \boldsymbol{d}_4^*$ denote the elements of $\mathbb{D}^*$. It also picks $\alpha \xleftarrow{R} \mathbb{Z}_q$ and outputs the public parameters as
$$\mathsf{PP} := \{\mathbb{G}; e(g_1, g_2)^{\alpha \boldsymbol{d}_1 \cdot \boldsymbol{d}_1^*}, g_1^{\boldsymbol{d}_1}, g_1^{\boldsymbol{d}_2}\},$$
and the master key
$$\mathsf{MK} := \{\alpha, g_2^{\boldsymbol{d}_1^*}, g_2^{\boldsymbol{d}_2^*}\}.$$
- $\mathsf{KeyGen}(\mathsf{PP}, \mathsf{MK}, ID)$ This algorithm picks $r \xleftarrow{R} \mathbb{Z}_q$. The secret key is computed as
$$\mathsf{SK}_{ID} := g_2^{(\alpha + rID)\boldsymbol{d}_1^* - r\boldsymbol{d}_2^*}.$$
- $\mathsf{Enc}(\mathsf{PP}, ID, M)$ This algorithm picks $s \xleftarrow{R} \mathbb{Z}_q$ and forms the ciphertext as
$$\mathsf{CT}_{ID} := \left\{ C_0 := M \cdot (e(g_1, g_2)^{\alpha \boldsymbol{d}_1 \cdot \boldsymbol{d}_1^*})^s, \quad C_1 := g_1^{s\boldsymbol{d}_1 + sID\boldsymbol{d}_2} \right\}.$$
- $\mathsf{Dec}(\mathsf{PP}, \mathsf{SK}_{ID}, \mathsf{CT}_{ID})$ This algorithm computes the message as
$$M := C_0 / e(C_1, \mathsf{SK}_{ID}).$$

Correctness. Correctness is straight-forward:

$$\begin{aligned} C_0/e(C_1, \mathsf{SK}_{ID}) &= M \cdot (e(g_1, g_2)^{\alpha \boldsymbol{d}_1 \cdot \boldsymbol{d}_1^*})^s / e(g_1^{s\boldsymbol{d}_1 + sID\boldsymbol{d}_2}, g_2^{(\alpha + rID)\boldsymbol{d}_1^* - r\boldsymbol{d}_2^*}) \\ &= M \cdot (e(g_1, g_2)^{\alpha \boldsymbol{d}_1 \cdot \boldsymbol{d}_1^*})^s / \big(e(g_1, g_2)^{\alpha s \boldsymbol{d}_1 \cdot \boldsymbol{d}_1^*} \\ &\qquad \cdot e(g_1, g_2)^{srID\boldsymbol{d}_1 \cdot \boldsymbol{d}_1^* - srID\boldsymbol{d}_2 \cdot \boldsymbol{d}_2^*}\big) \\ &= M \cdot (e(g_1, g_2)^{\alpha \boldsymbol{d}_1 \cdot \boldsymbol{d}_1^*})^s / e(g_1, g_2)^{\alpha s \boldsymbol{d}_1 \cdot \boldsymbol{d}_1^*} = M. \end{aligned}$$

Proof of Security. We prove the following theorem by showing a series of lemmas.

Theorem 1. *The IBE scheme is fully secure and anonymous under the Symmetric External Diffie-Hellman assumption. More precisely, for any adversary $\mathcal{A}$ against the IBE scheme, there exist probabilistic algorithms $\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_\nu$ whose running times are essentially the same as that of $\mathcal{A}$, such that*

$$\mathsf{Adv}^{\mathsf{IBE}}_{\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DDH1}}_{\mathcal{B}_0}(\lambda) + \sum_{\kappa=1}^{\nu} \mathsf{Adv}^{\mathsf{DDH2}}_{\mathcal{B}_\kappa}(\lambda) + \frac{\nu}{q}$$

where ν is the maximum number of $\mathcal{A}$'s key queries.

We adopt the dual system encryption methodology by Waters [36] to prove the security of our IBE scheme. We use the concepts of *semi-functional ciphertexts* and *semi-functional keys* in our proof and provide algorithms that generate them. We note that these algorithms are only provided for definitional purposes, and are not part of the IBE system. In particular, they do not need to be efficiently computable from the public parameters and the master key.

KeyGenSF The algorithm picks random values $r, t_3, t_4 \in \mathbb{Z}_q$ and forms a semi-functional secret key as

$$\mathsf{SK}^{(SF)}_{ID} := g_2^{(\alpha + rID)\boldsymbol{d}_1^* - r\boldsymbol{d}_2^* + t_3\boldsymbol{d}_3^* + t_4\boldsymbol{d}_4^*}.$$

EncryptSF The algorithm picks random values random values $s, z_3, z_4 \in \mathbb{Z}_q$ and forms a semi-functional ciphertext as

$$\mathsf{CT}^{(SF)}_{ID} := \Big\{ C_0 := M \cdot (e(g_1, g_2)^{\alpha \boldsymbol{d}_1 \cdot \boldsymbol{d}_1^*})^s, \quad C_1 := g_1^{s\boldsymbol{d}_1 + sID\boldsymbol{d}_2 + z_3\boldsymbol{d}_3 + z_4\boldsymbol{d}_4} \Big\}.$$

We observe that if one applies the decryption procedure with a semi-functional key and a normal ciphertext, decryption will succeed because $\boldsymbol{d}_3^*, \boldsymbol{d}_4^*$ are orthogonal to all of the vectors in exponent of C_1, and hence have no effect on decryption. Similarly, decryption of a semi-functional ciphertext by a normal key will also succeed because $\boldsymbol{d}_3, \boldsymbol{d}_4$ are orthogonal to all of the vectors in the exponent of the key. When both the ciphertext and key are semi-functional, the result of $e(C_1, \mathsf{SK}_{ID})$ will have an additional term, namely

$$e(g_1, g_2)^{t_3 z_3 \boldsymbol{d}_3^* \cdot \boldsymbol{d}_3 + t_4 z_4 \boldsymbol{d}_4^* \cdot \boldsymbol{d}_4} = e(g_1, g_2)^{(t_3 z_3 + t_4 z_4)\psi}.$$

Decryption will then fail unless $t_3 z_3 + t_4 z_4 \equiv 0 \bmod q$. If this modular equation holds, we say that the key and ciphertext pair is *nominally semi-functional*.

For a probabilistic polynomial-time adversary $\mathcal{A}$ which makes ν key queries $ID_1, \ldots, ID_\nu$, our proof of security consists of the following sequence of games between $\mathcal{A}$ and a challenger $\mathcal{B}$.

- Game_{Real}: is the real security game.

– Game_0: is the same as Game_{Real} except that the challenge ciphertext is semi-functional.
– Game_κ: for κ from 1 to ν, Game_κ is the same as Game_0 except that the first κ keys are semi-functional and the remaining keys are normal.
– Game_{Final}: is the same as Game_ν, except that the challenge ciphertext is a semi-functional encryption of a random message in G_T and under a random identity in $\mathbb{Z}_q$. We denote the challenge ciphertext in Game_{Final} as $\mathsf{CT}^{(R)}_{ID_R}$.

We prove following lemmas to show the above games are indistinguishable by following an analogous strategy of [25]. Our main arguments are computational indistinguishability (guaranteed by the Subspace assumptions, which are implied by the SXDH assumption) and statistical indistinguishability. The advantage gap between Game_{Real} and Game_0 is bounded by the advantage of the Subspace assumption in G_1. Additionally, we require a statistical indistinguishability argument to show that the distribution of the challenge ciphertext remains the same from the adversary's view. For κ from 1 to ν, the advantage gap between $\mathsf{Game}_{\kappa-1}$ and Game_κ is bounded by the advantage of Subspace assumption in G_2. Similarly, we require a statistical indistinguishability argument to show that the distribution of the the κ-th semi-functional key remains the same from the adversary's view. Finally, we statistically transform Game_ν to Game_{Final} in one step, i.e., we show the joint distributions of

$$(\mathsf{PP}, \mathsf{CT}^{(SF)}_{ID^*_\beta}, \{\mathsf{SK}^{(SF)}_{ID_\ell}\}_{\ell=1,\ldots,\nu}) \text{ and } (\mathsf{PP}, \mathsf{CT}^{(R)}_{ID_R}, \{\mathsf{SK}^{(SF)}_{ID_\ell}\}_{\ell=1,\ldots,\nu})$$

are equivalent for the adversary's view.

We let $\mathsf{Adv}^{\mathsf{Game}_{Real}}_{\mathcal{A}}$ denote an adversary $\mathcal{A}$'s advantage in the real game.

Lemma 3. *Suppose that there exists an adversary $\mathcal{A}$ where $|\mathsf{Adv}^{\mathsf{Game}_{Real}}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{\mathsf{Game}_0}_{\mathcal{A}}(\lambda)| = \epsilon$. Then there exists an algorithm $\mathcal{B}_0$ such that $\mathsf{Adv}^{\mathsf{DS1}}_{\mathcal{B}_0}(\lambda) = \epsilon$, with $k = 2$ and $n = 4$.*

Proof. $\mathcal{B}_0$ is given

$$D := (\mathbb{G}; g_2^{\boldsymbol{b}^*_1}, g_2^{\boldsymbol{b}^*_2}, g_1^{\boldsymbol{b}_1}, \ldots, g_1^{\boldsymbol{b}_4}, U_1, U_2, \mu_2).$$

along with T_1, T_2. We require that $\mathcal{B}_0$ decides whether T_1, T_2 are distributed as $g_1^{\tau_1 \boldsymbol{b}_1}, g_1^{\tau_1 \boldsymbol{b}_2}$ or $g_1^{\tau_1 \boldsymbol{b}_1 + \tau_2 \boldsymbol{b}_3}, g_1^{\tau_1 \boldsymbol{b}_2 + \tau_2 \boldsymbol{b}_4}$.

$\mathcal{B}_0$ simulates Game_{Real} or Game_0 with $\mathcal{A}$, depending on the distribution of T_1, T_2. To compute the public parameters and master secret key, $\mathcal{B}_0$ first chooses a random invertible matrix $A \in \mathbb{Z}_q^{2\times 2}$ (A is invertible with overwhelming probability if it is uniformly picked). We implicitly set dual orthonormal bases $\mathbb{D}, \mathbb{D}^*$ to:

$$\begin{aligned} \boldsymbol{d}_1 &:= \boldsymbol{b}_1, \quad \boldsymbol{d}_2 := \boldsymbol{b}_2, \quad (\boldsymbol{d}_3, \boldsymbol{d}_4) := (\boldsymbol{b}_3, \boldsymbol{b}_4)A, \\ \boldsymbol{d}^*_1 &:= \boldsymbol{b}^*_1, \quad \boldsymbol{d}^*_2 := \boldsymbol{b}^*_2, \quad (\boldsymbol{d}^*_3, \boldsymbol{d}^*_4) := (\boldsymbol{b}^*_3, \boldsymbol{b}^*_4)(A^{-1})^t. \end{aligned}$$

We note that $\mathbb{D}, \mathbb{D}^*$ are properly distributed, and reveal no information about A. Moreover, $\mathcal{B}_0$ cannot generate $g_2^{\boldsymbol{d}^*_3}, g_2^{\boldsymbol{d}^*_4}$, but these will not be needed for creating normal keys. $\mathcal{B}_0$ chooses random value $\alpha \in \mathbb{Z}_q$ and computes $e(g_1, g_2)^{\alpha \boldsymbol{d}_1 \cdot \boldsymbol{d}^*_1}$. It then gives $\mathcal{A}$ the public parameters

$$\mathsf{PP} := \{\mathbb{G}; e(g_1, g_2)^{\alpha \boldsymbol{d}_1 \cdot \boldsymbol{d}^*_1}, g_1^{\boldsymbol{d}_1}, g_1^{\boldsymbol{d}_2}\}.$$

The master key

$$\mathsf{MK} := \{\alpha, g_2^{\boldsymbol{d}^*_1}, g_2^{\boldsymbol{d}^*_2}\}$$

is known to $\mathcal{B}_0$, which allows $\mathcal{B}_0$ to respond to all of $\mathcal{A}$'s key queries by calling the normal key generation algorithm.

$\mathcal{A}$ sends $\mathcal{B}_0$ two pairs (M_0, ID_0^*) and (M_1, ID_1^*). $\mathcal{B}_0$ chooses a random bit $\beta \in \{0,1\}$ and encrypts M_β under ID_β^* as follows:

$$C_0 := M_\beta \Big(e(T_1, g_2^{\boldsymbol{b}_1^*}) \Big)^\alpha = M_\beta \Big(e(g_1, g_2)^{\alpha \boldsymbol{d}_1 \boldsymbol{d}_1^*} \Big)^s, \quad C_1 := T_1 (T_2)^{ID_\beta^*},$$

where $\mathcal{B}_0$ has implicitly set $s := \tau_1$. It gives the ciphertext $\mathsf{CT}_{ID_\beta^*}$ to $\mathcal{A}$.

Now, if T_1, T_2 are equal to $g_1^{\tau_1 \boldsymbol{b}_1}, g_1^{\tau_1 \boldsymbol{b}_2}$, then this is a properly distributed normal encryption of M_β. In this case, $\mathcal{B}_0$ has properly simulated Game_{Real}. If T_1, T_2 are equal to $g_1^{\tau_1 \boldsymbol{b}_1 + \tau_2 \boldsymbol{b}_3}, g_1^{\tau_1 \boldsymbol{b}_2 + \tau_2 \boldsymbol{b}_4}$ instead, then the ciphertext element C_1 has an additional term of

$$\tau_2 \boldsymbol{b}_3 + ID_\beta^* \tau_2 \boldsymbol{b}_4$$

in its exponent. The coefficients here in the basis $\boldsymbol{b}_3, \boldsymbol{b}_4$ form the vector $\tau_2, ID_\beta^* \tau_2$. To compute the coefficients in the basis $\boldsymbol{d}_3, \boldsymbol{d}_4$, we multiply the matrix A^{-1} by the transpose of this vector, obtaining $\tau_2 A^{-1} (1, ID_\beta^*)^t$. Since A is random (everything else given to $\mathcal{A}$ has been distributed independently of A), these coefficients are uniformly random from Lemma 1. Therefore, in this case, $\mathcal{B}_0$ has properly simulated Game_0. This allows $\mathcal{B}_0$ to leverage $\mathcal{A}$'s advantage ϵ between Game_{Real} and Game_0 to achieve an advantage ϵ against the Subspace assumption in G_1, namely $\mathsf{Adv}_{\mathcal{B}_0}^{\mathsf{DS1}}(\lambda) = \epsilon$. □

Lemma 4. *Suppose that there exists an adversary $\mathcal{A}$ where $|\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_{\kappa-1}}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_\kappa}(\lambda)| = \epsilon$. Then there exists an algorithm $\mathcal{B}_\kappa$ such that $\mathsf{Adv}_{\mathcal{B}_\kappa}^{\mathsf{DS2}}(\lambda) = \epsilon - 1/q$, with $k = 2$ and $n = 4$.*

Proof. $\mathcal{B}_\kappa$ is given

$$D := (\mathbb{G}; g_1^{\boldsymbol{b}_1}, g_1^{\boldsymbol{b}_2}, g_2^{\boldsymbol{b}_1^*}, \ldots, g_2^{\boldsymbol{b}_4^*}, U_1, U_2, \mu_2)$$

along with T_1, T_2. We require that $\mathcal{B}_\kappa$ decides whether T_1, T_2 are distributed as $g_2^{\tau_1 \boldsymbol{b}_1^*}, g_2^{\tau_1 \boldsymbol{b}_2^*}$ or $g_2^{\tau_1 \boldsymbol{b}_1^* + \tau_2 \boldsymbol{b}_3^*}, g_2^{\tau_1 \boldsymbol{b}_2^* + \tau_2 \boldsymbol{b}_4^*}$.

$\mathcal{B}_\kappa$ simulates Game_κ or $\mathsf{Game}_{\kappa-1}$ with $\mathcal{A}$, depending on the distribution of T_1, T_2. To compute the public parameters and master secret key, $\mathcal{B}_\kappa$ chooses a random matrix $A \in \mathbb{Z}_q^{2\times 2}$ (with all but negligible probability, A is invertible). We then implicitly set dual orthonormal bases $\mathbb{D}, \mathbb{D}^*$ to:

$$\begin{aligned} \boldsymbol{d}_1 &:= \boldsymbol{b}_1, \quad \boldsymbol{d}_2 := \boldsymbol{b}_2, \quad (\boldsymbol{d}_3, \boldsymbol{d}_4) := (\boldsymbol{b}_3, \boldsymbol{b}_4) A, \\ \boldsymbol{d}_1^* &:= \boldsymbol{b}_1^*, \quad \boldsymbol{d}_2^* := \boldsymbol{b}_2^*, \quad (\boldsymbol{d}_3^*, \boldsymbol{d}_4^*) := (\boldsymbol{b}_3^*, \boldsymbol{b}_4^*)(A^{-1})^t. \end{aligned}$$

We note that $\mathbb{D}, \mathbb{D}^*$ are properly distributed, and reveal no information about A. $\mathcal{B}_\kappa$ chooses random value $\alpha \in \mathbb{Z}_q$ and compute $e(g_1, g_2)^{\alpha \boldsymbol{d}_1 \cdot \boldsymbol{d}_1^*}$. $\mathcal{B}_\kappa$ can gives $\mathcal{A}$ the public parameters

$$\mathsf{PP} := \{\mathbb{G}; e(g_1, g_2)^{\alpha \boldsymbol{d}_1 \cdot \boldsymbol{d}_1^*}, g_1^{\boldsymbol{d}_1}, g_1^{\boldsymbol{d}_2}\}.$$

The master key

$$\mathsf{MK} := \{\alpha, g_2^{\boldsymbol{d}_1^*}, g_2^{\boldsymbol{d}_2^*}\}$$

is known to $\mathcal{B}_\kappa$, which allows $\mathcal{B}_\kappa$ to respond to all of $\mathcal{A}$'s key queries by calling the normal key generation algorithm. Since $\mathcal{B}_\kappa$ also knows $g_2^{\boldsymbol{d}_3^*}$ and $g_2^{\boldsymbol{d}_4^*}$, it can easily produce semi-functional keys. To answer the first $\kappa - 1$ key queries that $\mathcal{A}$ makes, $\mathcal{B}_\kappa$ runs the semi-functional key generation

algorithm to produce semi-functional keys and gives these to $\mathcal{A}$. To answer the κ-th key query for ID_κ, $\mathcal{B}_\kappa$ responds with:

$$\mathsf{SK}_{ID_\kappa} := (g_2^{\boldsymbol{b}_1^*})^\alpha T_1^{ID_\kappa} (T_2)^{-1}.$$

This implicitly sets $r := \tau_1$. If T_1, T_2 are equal to $g_2^{\tau_1 \boldsymbol{b}_1^*}, g_2^{\tau_1 \boldsymbol{b}_2^*}$, then this is a properly distributed normal key. If T_1, T_2 are equal to $g_2^{\tau_1 \boldsymbol{b}_1^* + \tau_2 \boldsymbol{b}_3^*}, g_2^{\tau_1 \boldsymbol{b}_2^* + \tau_2 \boldsymbol{b}_4^*}$, then this is a semi-functional key, whose exponent vector includes

$$ID_\kappa \tau_2 \boldsymbol{b}_3^* - \tau_2 \boldsymbol{b}_4^* \tag{1}$$

as its component in the span of $\boldsymbol{b}_3^*, \boldsymbol{b}_4^*$. To respond to the remaining key queries, $\mathcal{B}_\kappa$ simply runs the normal key generation algorithm.

At some point, $\mathcal{A}$ sends $\mathcal{B}_\kappa$ two pairs (M_0, ID_0^*) and (M_1, ID_1^*). $\mathcal{B}_\kappa$ chooses a random bit $\beta \in \{0,1\}$ and encrypts M_β under ID_β^* as follows:

$$C_0 := M_\beta \Big(e(U_1, g_2^{\boldsymbol{b}_1^*}) \Big)^\alpha = M_\beta \Big(e(g_1, g_2)^{\alpha \boldsymbol{d}_1 \boldsymbol{d}_1^*} \Big)^s, \quad C_1 := U_1 (U_2)^{ID_\beta^*},$$

where $\mathcal{B}_\kappa$ has implicitly set $s := \mu_1$. The "semi-functional part" of the exponent vector here is:

$$\mu_2 \boldsymbol{b}_3 + ID^* \mu_2 \boldsymbol{b}_4. \tag{2}$$

We observe that if $ID_\beta^* = ID_\kappa$ (which is not allowed), then vectors 1 and 2 would be orthogonal, resulting in a nominally semi-functional ciphertext and key pair. It gives the ciphertext $\mathsf{CT}_{ID_\beta^*}$ to $\mathcal{A}$.

We now argue that since $ID_\beta^* \neq ID_\kappa$, in $\mathcal{A}$'s view the vectors 1 and 2 are distributed as random vectors in the spans of $\boldsymbol{d}_3^*, \boldsymbol{d}_4^*$ and $\boldsymbol{d}_3, \boldsymbol{d}_4$ respectively. To see this, we take the coefficients of vectors 1 and 2 in terms of the bases $\boldsymbol{b}_3^*, \boldsymbol{b}_4^*$ and $\boldsymbol{b}_3, \boldsymbol{b}_4$ respectively and translate them into coefficients in terms of the bases $\boldsymbol{d}_3^*, \boldsymbol{d}_4^*$ and $\boldsymbol{d}_3, \boldsymbol{d}_4$. Using the change of basis matrix A, we obtain the new coefficients (in vector form) as:

$$\tau_2 A^t (ID_\kappa, -1)^t,\ \mu_2 A^{-1} (1, ID_\beta^*).$$

Since the distribution of everything given to A except for the κ-th key and the challenge ciphertext is independent of the random matrix A and $ID_\beta^* \neq ID_\kappa$, we can conclude that these coefficients are uniformly random (except for $1/q$ probability) from Lemma 1. Thus, $\mathcal{B}_\kappa$ has properly simulated Game_κ in this case.

In summary, $\mathcal{B}_\kappa$ has properly simulated either $\mathsf{Game}_{\kappa-1}$ or Game_κ for $\mathcal{A}$, depending on the distribution of T_1, T_2. It can therefore leverage $\mathcal{A}$'s advantage ϵ between these games to obtain an advantage $\epsilon - 1/q$ against the Subspace assumption in G_2, namely $\mathsf{Adv}^{\mathsf{DS2}}_{\mathcal{B}_\kappa}(\lambda) = \epsilon - 1/q$. □

Lemma 5. *For any adversary $\mathcal{A}$, $\mathsf{Adv}^{\mathsf{Game}_\nu}_{\mathcal{A}}(\lambda) = \mathsf{Adv}^{\mathsf{Game}_{Final}}_{\mathcal{A}}(\lambda)$.*

Proof. To prove this lemma, we show the joint distributions of

$$(\mathsf{PP}, \mathsf{CT}^{(SF)}_{ID_\beta^*}, \{\mathsf{SK}^{(SF)}_{ID_\ell}\}_{\ell=1,\ldots,\nu})$$

in Game_ν and that of

$$(\mathsf{PP}, \mathsf{CT}^{(R)}_{ID_R}, \{\mathsf{SK}^{(SF)}_{ID_\ell}\}_{\ell=1,\ldots,\nu})$$

in Game_{Final} are equivalent for the adversary's view, where $\mathsf{CT}^{(R)}_{ID_R}$ is a semi-functional encryption of a random message in G_T and under a random identity in $\mathbb{Z}_q$.

For this purpose, we pick $A := (\xi_{i,j}) \xleftarrow{R} \mathbb{Z}_q^{2\times 2}$ and define new dual orthonormal bases $\mathbb{F} := (\boldsymbol{f}_1, \ldots, \boldsymbol{f}_4)$, and $\mathbb{F}^* := (\boldsymbol{f}^*_1, \ldots, \boldsymbol{f}^*_4)$ as follows:

$$\begin{pmatrix} \boldsymbol{f}_1 \\ \boldsymbol{f}_2 \\ \boldsymbol{f}_3 \\ \boldsymbol{f}_4 \end{pmatrix} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \xi_{1,1} & \xi_{1,2} & 1 & 0 \\ \xi_{2,1} & \xi_{2,2} & 0 & 1 \end{pmatrix} \begin{pmatrix} \boldsymbol{d}_1 \\ \boldsymbol{d}_2 \\ \boldsymbol{d}_3 \\ \boldsymbol{d}_4 \end{pmatrix}, \quad \begin{pmatrix} \boldsymbol{f}^*_1 \\ \boldsymbol{f}^*_2 \\ \boldsymbol{f}^*_3 \\ \boldsymbol{f}^*_4 \end{pmatrix} := \begin{pmatrix} 1 & 0 & -\xi_{1,1} & -\xi_{2,1} \\ 0 & 1 & -\xi_{1,2} & -\xi_{2,2} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \boldsymbol{d}^*_1 \\ \boldsymbol{d}^*_2 \\ \boldsymbol{d}^*_3 \\ \boldsymbol{d}^*_4 \end{pmatrix}.$$

It is easy to verify that $\mathbb{F}$ and $\mathbb{F}^*$ are also dual orthonormal, and are distributed the same as $\mathbb{D}$ and $\mathbb{D}^*$.

Then the public parameters, challenge ciphertext, and queried secret keys $(\mathsf{PP}, \mathsf{CT}^{(SF)}_{ID^*_\beta}, \{\mathsf{SK}^{(SF)}_{ID_\ell}\}_{\ell=1,\ldots,\nu})$ in Game_ν are expressed over bases $\mathbb{D}$ and $\mathbb{D}^*$ as

$$\begin{aligned}
&\mathsf{PP} := \{\mathbb{G}; e(g_1,g_2)^{\alpha \boldsymbol{d}_1 \cdot \boldsymbol{d}^*_1}, g_1^{\boldsymbol{d}_1}, g_1^{\boldsymbol{d}_2}\}, \\
&\mathsf{CT}^{(SF)}_{ID^*_\beta} := \left\{ C_0 := M \cdot (e(g_1,g_2)^{\alpha \boldsymbol{d}_1 \cdot \boldsymbol{d}^*_1})^s, \quad C_1 := g_1^{s\boldsymbol{d}_1 + sID^*_\beta \boldsymbol{d}_2 + z_3 \boldsymbol{d}_3 + z_4 \boldsymbol{d}_4} \right\}, \\
&\left\{ \mathsf{SK}^{(SF)}_{ID_\ell} := g_2^{(\alpha + r_\ell ID_\ell)\boldsymbol{d}^*_1 - r_\ell \boldsymbol{d}^*_2 + t_{\ell,3}\boldsymbol{d}^*_3 + t_{\ell,4}\boldsymbol{d}^*_4} \right\}_{\ell=1,\ldots,\nu}.
\end{aligned}$$

Then we can express them over bases $\mathbb{F}$ and $\mathbb{F}^*$ as

$$\begin{aligned}
&\mathsf{PP} := \{\mathbb{G}; e(g_1,g_2)^{\alpha \boldsymbol{f}_1 \cdot \boldsymbol{f}^*_1}, g_1^{\boldsymbol{f}_1}, g_1^{\boldsymbol{f}_2}\}, \\
&\mathsf{CT}^{(SF)}_{ID^*_\beta} := \left\{ C_0 := M \cdot (e(g_1,g_2)^{\alpha \boldsymbol{f}_1 \cdot \boldsymbol{f}^*_1})^s, \quad C_1 := g_1^{s'\boldsymbol{f}_1 + s''\boldsymbol{f}_2 + z_3 \boldsymbol{f}_3 + z_4 \boldsymbol{f}_4} \right\}, \\
&\left\{ \mathsf{SK}^{(SF)}_{ID_\ell} := g_2^{(\alpha + r_\ell ID_\ell)\boldsymbol{f}^*_1 - r_\ell \boldsymbol{f}^*_2 + t'_{\ell,3}\boldsymbol{f}^*_3 + t'_{\ell,4}\boldsymbol{f}^*_4} \right\}_{\ell=1,\ldots,\nu},
\end{aligned}$$

where

$$\begin{aligned}
&s' := s - z_3\xi_{1,1} - z_4\xi_{2,1}, \quad s'' := sID^*_\beta - z_3\xi_{1,2} - z_4\xi_{2,2}, \\
&\left\{ \begin{matrix} t'_{\ell,3} := t_{\ell,3} + \xi_{1,1}(\alpha + r_\ell ID_\ell) - r_\ell \xi_{1,2}, \\ t'_{\ell,4} := t_{\ell,4} + \xi_{2,1}(\alpha + r_\ell ID_\ell) - r_\ell \xi_{2,2} \end{matrix} \right\}_{\ell=1,\ldots,\nu},
\end{aligned}$$

which are all uniformly distributed since $\xi_{1,1}, \xi_{1,2}, \xi_{2,1}, \xi_{2,2}, t_{1,3}, t_{1,4}, \ldots, t_{\nu,3}, t_{\nu,4}$ are all uniformly picked from $\mathbb{Z}_q$.

In other words, the coefficients (s, sID^*_β) of $\boldsymbol{d}_1, \boldsymbol{d}_2$ in the C_1 term of the challenge ciphertext is changed to random coefficients $(s', s'') \in \mathbb{Z}_q \times \mathbb{Z}_q$ of $\boldsymbol{f}_1, \boldsymbol{f}_2$, thus the challenge ciphertext can be viewed as a semi-functional encryption of a random message in G_T and under a random identity in $\mathbb{Z}_q$. Moreover, all coefficients $\{(t'_{\ell,3}, t'_{\ell,4})\}_{\ell=1,\ldots,\nu}$ of $\boldsymbol{f}_1, \boldsymbol{f}_2$ in the $\{\mathsf{SK}^{(SF)}_{ID_\ell}\}_{\ell=1,\ldots,\nu}$ are all uniformly distributed since $\{(t_{\ell,3}, t_{\ell,4})\}_{\ell=1,\ldots,\nu}$ of $\boldsymbol{d}^*_3, \boldsymbol{d}^*_4$ are all independent random values. Thus

$$(\mathsf{PP}, \mathsf{CT}^{(SF)}_{ID^*_\beta}, \{\mathsf{SK}^{(SF)}_{ID_\ell}\}_{\ell=1,\ldots,\nu})$$

expressed over bases $\mathbb{F}$ and $\mathbb{F}^*$ is properly distributed as

$$(\mathsf{PP}, \mathsf{CT}^{(R)}_{ID_R}, \{\mathsf{SK}^{(SF)}_{ID_\ell}\}_{\ell=1,\ldots,\nu})$$

in Game_{Final}.

In the adversary's view, both $(\mathbb{D}, \mathbb{D}^*)$ and $(\mathbb{F}, \mathbb{F}^*)$ are consistent with the same public key. Therefore, the challenge ciphertext and queried secret keys above can be expressed as keys and ciphertext in two ways, in Game_ν over bases $(\mathbb{D}, \mathbb{D}^*)$ and in Game_{Final} over bases $(\mathbb{F}, \mathbb{F}^*)$. Thus, Game_ν and Game_{Final} are statistically indistinguishable. □

Lemma 6. *For any adversary $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_{Final}}(\lambda) = 0$.*

Proof. The value of β is independent from the adversary's view in Game_{Final}. Hence, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_{Final}}(\lambda) = 0$. □

In Game_{Final}, the challenge ciphertext is a semi-functional encryption of a random message in G_T and under a random identity in $\mathbb{Z}_q$, independent of the two messages and the challenge identities provided by $\mathcal{A}$. Thus, our IBE scheme is anonymous.

5 A Signature Scheme

In this section, we present the signature scheme derived from the preceding IBE scheme via Naor's transform. The security of the signature scheme follows from the full security of our IBE scheme.

- $\mathsf{KeyGen}(1^\lambda)$ This algorithm takes in the security parameter λ and generates a bilinear pairing $\mathbb{G} := (q, G_1, G_2, G_T, g_1, g_2, e)$ for sufficiently large prime order q. The algorithm samples random dual orthonormal bases, $(\mathbb{D}, \mathbb{D}^*) \xleftarrow{R} \mathsf{Dual}(\mathbb{Z}_q^4)$. Let $\boldsymbol{d}_1, \ldots, \boldsymbol{d}_4$ denote the elements of $\mathbb{D}$ and $\boldsymbol{d}_1^*, \ldots, \boldsymbol{d}_4^*$ denote the elements of $\mathbb{D}^*$. It outputs the public key as

$$\mathsf{PK} = \{\mathbb{G}; e(g_1, g_2)^{\alpha \boldsymbol{d}_1 \cdot \boldsymbol{d}_1^*}, g_1^{\boldsymbol{d}_1}, g_1^{\boldsymbol{d}_2}\},$$

  and the signing key

$$\mathsf{SK} = \{\alpha, g_2^{\boldsymbol{d}_1^*}, g_2^{\boldsymbol{d}_2^*}\}.$$

- $\mathsf{Sign}(\mathsf{PK}, \mathsf{SK}, M)$ This algorithm picks $r \xleftarrow{R} \mathbb{Z}_q$ and computes the signature as

$$\sigma = g_2^{(\alpha + rM)\boldsymbol{d}_1^* - r\boldsymbol{d}_2^*}.$$

- $\mathsf{Verify}(\mathsf{PK}, \sigma, M)$ This algorithm verifies a signature σ by testing whether $e(g_1^{\boldsymbol{d}_1 + M\boldsymbol{d}_2}, \sigma) = e(g_1, g_2)^{\alpha \boldsymbol{d}_1 \cdot \boldsymbol{d}_1^*}$.[3] If the equality holds the signature is declared `valid`; otherwise it is declared `invalid`.

Acknowledgments. We thank the referees for helpful feedback.

[3] Directly applying Naor's transform yields a verification algorithm that works as follows: pick $s \leftarrow \mathbb{Z}_q$, and test whether $e(g_1^{(\boldsymbol{d}_1 + M\boldsymbol{d}_2)s}, \sigma) = (e(g_1, g_2)^{\alpha \boldsymbol{d}_1 \cdot \boldsymbol{d}_1^*})^s$. With overwhelming probability over s, this agrees with the verification algorithm as written.

References

[1] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi. Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. *J. Cryptology*, 21(3):350–391, 2008.

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

[3] G. Ateniese, J. Kirsch, and M. Blanton. Secret handshakes with dynamic and fuzzy matching. In *NDSS*, 2007.

[4] L. Ballard, M. Green, B. de Medeiros, and F. Monrose. Correlation-resistant storage via keyword-searchable encryption. IACR Cryptology ePrint Archive, Report 2005/417, 2005.

[5] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid. Recommendation for key management—part 1: General (revised). *NIST Special Pub*, 800-57, 2007.

[6] P. S. L. M. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order. In *Selected Areas in Cryptography*, pages 319–331, 2005.

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

[8] D. Boneh and X. Boyen. Secure identity based encryption without random oracles. In *CRYPTO*, pages 443–459, 2004.

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

[10] D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In *CRYPTO*, pages 41–55, 2004.

[11] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. *J. Cryptology*, 17(4):297–319, 2004.

[12] Z. Brakerski, Y. T. Kalai, J. Katz, and V. Vaikuntanathan. Overcoming the hole in the bucket: Public-key cryptography resilient to continual memory leakage. In *FOCS*, pages 501–510, 2010.

[13] F. Brezing and A. Weng. Elliptic curves suitable for pairing based cryptography. *Des. Codes Cryptography*, 37(1):133–141, 2005.

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

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

[16] C. Cocks. An identity based encryption scheme based on quadratic residues. In *IMA Int. Conf.*, pages 360–363, 2001.

[17] L. Ducas. Anonymity from asymmetry: New constructions for anonymous HIBE. In *CT-RSA*, pages 148–164, 2010.

[18] D. Freeman, M. Scott, and E. Teske. A taxonomy of pairing-friendly elliptic curves. *J. Cryptology*, 23(2):224–280, 2010.

[19] D. M. Freeman. Converting pairing-based cryptosystems from composite-order groups to prime-order groups. In *EUROCRYPT*, pages 44–61, 2010.

[20] S. D. Galbraith and V. Rotger. Easy decision Diffie-Hellman groups. IACR Cryptology ePrint Archive, Report 2004/070, 2004.

[21] C. Gentry. Practical identity-based encryption without random oracles. In *EUROCRYPT*, pages 445–464, 2006.

[22] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *STOC*, pages 197–206, 2008.
[23] S. Goldwasser, S. Micali, and R. L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM J. Comput.*, 17(2):281–308, 1988.
[24] J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In *EUROCRYPT*, pages 415–432, 2008.
[25] A. Lewko. Tools for simulating features of composite order bilinear groups in the prime order setting. In *EUROCRYPT*, 2012.
[26] 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.
[27] 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.
[28] A. Miyaji, M. Nakabayashi, and S. Takano. Characterization of elliptic curve traces under fr-reduction. In *ICISC*, pages 90–108, 2000.
[29] T. Okamoto and K. Takashima. Homomorphic encryption and signatures from vector decomposition. In *Pairing*, pages 57–74, 2008.
[30] T. Okamoto and K. Takashima. Hierarchical predicate encryption for inner-products. In *ASIACRYPT*, pages 214–231, 2009.
[31] T. Okamoto and K. Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In *CRYPTO*, pages 191–208, 2010. Also, Cryptology ePrint Archive, Report 2010/563.
[32] S. C. Ramanna, S. Chatterjee, and P. Sarkar. Variants of waters' dual-system primitives using asymmetric pairings. IACR Cryptology ePrint Archive, Report 2012/024, 2012.
[33] A. Shamir. Identity-based cryptosystems and signature schemes. In *CRYPTO*, pages 47–53, 1984.
[34] E. R. Verheul. Evidence that XTR is more secure than Supersingular Elliptic Curve cryptosystems. *Journal of Cryptology*, 17(4):277–296, 2004.
[35] B. Waters. Efficient identity-based encryption without random oracles. In *EUROCRYPT*, pages 114–127, 2005.
[36] B. Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In *CRYPTO*, pages 619–636, 2009.

A Estimated Bit Sizes of Group Elements for Bilinear Group Generators

The ordinary elliptic curves that give the best performance while providing discrete log security comparable to three commonly proposed levels of AES security are as follows. The group sizes follow the 2007 NIST recommendations [5], descriptions of the elliptic curves are in [18].

80-bit security : A 170-bit MNT curve [28] with embedding degree $k = 6$.
128-bit security : A 256-bit Barreto-Naehrig curve [6] with $k = 12$.
256-bit security : A 640-bit Brezing-Weng curve [13] with $k = 24$.

Note that a symmetric pairing only exists on supersingular elliptic curves. The restriction to supersingular elliptic curves means that at high security levels the group G_1 will be much larger than the group G_1 on an equivalent ordinary curve.

Pairings	80-bit AES			128-bit AES			256-bit AES		
	G_1	G_2	G_T	G_1	G_2	G_T	G_1	G_2	G_T
Asymmetric	170	340	1020	256	512	3072	640	2560	15360
Symmetric	176	176	1056	512	512	3072	2560	2560	15360

Table 2. Estimated bit sizes of elements in bilinear groups.