Identity-Based Matchmaking Encryption from Standard Assumptions

Jie Chen[1(✉)], Yu Li[1], Jinming Wen[2,3], and Jian Weng[2]

[1] Shanghai Key Laboratory of Trustworthy Computing, Software Engineering Institute, East China Normal University, Shanghai 200062, China
`s080001@e.ntu.edu.sg, yli@stu.ecnu.edu.cn`

[2] College of Information Science and Technology and the College of Cyber Security, Jinan University, Guangzhou 510632, China
`jinming.wen@mail.mcgill.ca, cryptjweng@gmail.com`

[3] State Key Laboratory of Cryptology, P.O. Box 5159, Beijing, 100878, China

Abstract. In this work, we propose the first identity-based matchmaking encryption (IB-ME) scheme under the standard assumptions in the standard model. This scheme is proven to be secure under the symmetric external Diffie-Hellman (SXDH) assumption in prime order bilinear pairing groups. In our IB-ME scheme, all parameters have constant number of group elements and are simpler than those of previous constructions. Previous works are either in the random oracle model or based on the q-type assumptions, while ours is built directly in the standard model and based on static assumptions, and does not rely on other crypto tools.

More concretely, our IB-ME scheme is constructed from a variant of two-level anonymous IBE. We observed that this two-level IBE with anonymity and unforgeability satisfies the same functionality of IB-ME, and its security properties cleverly meet the two requirements of IB-ME (Privacy and Authenticity). The privacy property of IB-ME relies on the anonymity of this two-level IBE, while the authenticity property is corresponding to the unforgeability in the 2nd level. This variant of two-level IBE is built from dual pairing vector spaces, and both security reductions rely on dual system encryption.

Keywords: Matchmaking encryption · Identity-based encryption · Standard assumptions · Standard model

1 Introduction

Matchmaking Encryption (ME) is a new form of encryption proposed by Ateniese et al. [3] in Crypto 2019, in which both the sender and the receiver (each with its own attributes) can specify fine-grained access policies the other party must satisfy in order for the message to be revealed. Using ME, a sender with attributes $\sigma \in \{0,1\}^*$ encrypts messages after generating the policy $\mathbb{R}$ of the intended receiver, and a receiver with attributes $\rho \in \{0,1\}^*$ obtains a decryption key $dk_{\mathbb{S}}$ from an authority before decrypting the ciphertext from a sender satisfying the specified policy $\mathbb{S}$. This receiver will correctly decrypt the ciphertext and obtain the message if and only if the sender's attributes σ match the policy $\mathbb{S}$ specified by the receiver, and at the same time the receiver's attributes ρ match the policy $\mathbb{R}$ specified by the sender. The implementation of matchmaking encryption in an identity-based setting is dubbed identity-based matchmaking encryption (IB-ME), where both the sender and the receiver specify a single identity instead of general policies.

Differently from ME, each identity is chosen by the sender or receiver on the fly without talking to the authority in an identity-based setting. Now each identity $x \in \{0,1\}^*$ will represent an access policy $\mathbb{A}$, which means that we use snd and rcv to represent the target policies $\mathbb{S}$ and $\mathbb{R}$ specified by the receiver and the sender, respectively. The sender's identity $\sigma \in \{0,1\}^*$ and its target policies rcv can be embedded in the ciphertext. The receiver with an identity ρ can now additionally specify a target identity $\mathsf{snd} \in \{0,1\}^*$ on the fly, and obtain the correct message as long as the sender's identity σ match the receiver's policy snd and vice-versa (i.e., $\rho = \mathsf{rcv}$ and $\sigma = \mathsf{snd}$). From this perspective, IB-ME can be considered as a more expressive version and generalization of anonymous identity-based encryption, in which both the sender and the receiver can specify a target communicating entity in a privacy-preserving manner.

Ateniese et al. [3] provide generic frameworks for constructing ME from functional encryption and propose the first IB-ME scheme with provable security under the bilinear Diffie-Hellman (BDH) assumption, but in the random oracle model. They also deploy experiments to prove their construction is practical and created an anonymous bulletin board over a Tor network. Following their work, Francati et al. [16] give the first IB-ME construction satisfying privacy in the plain model (without random oracles), but based on q-ABDHE assumption and non-interactive zero-knowledge (NIZK) proof systems. Meanwhile, they exhibit a generic transform taking as input any private IB-ME and outputting an IB-ME satisfying both enhanced privacy and authenticity. These leave the following problem:

Can we construct IB-ME under the standard assumptions
in the standard model?

1.1 Our Results

In this work, we present the first IB-ME scheme under the standard assumptions in the standard model. This scheme is based on the SXDH assumption in prime order bilinear pairing groups. The construction is direct and does not rely on other cryptographic tools such as non-interactive zero-knowledge proof systems. We summarize existing IB-ME schemes in Table 1 and several salient features of this work from the following two aspects:

– First, we adopt a variant of two-level IBE with anonymity modified from Chen's anonymous IBE and signature scheme [13] to form our construction. This two-level IBE with anonymity and unforgeability satisfies the same

Reference	Model	Assumption
AFNV19 [3]	Random Oracle	BDH
FGRV21 [16]	Standard	q-ABDHE+NIZK
Ours	Standard	SXDH

Table 1. Comparison with existing IB-ME schemes

functionality of IB-ME, and its security properties cleverly meet the two requirements of IB-ME (privacy and authenticity). The privacy property of IB-ME relies on the anonymity of the 1st level IBE, while the authenticity property is corresponding to the unforgeability in the 2nd level. The usage of this variant of two-level anonymous IBE allows our scheme to technically ensure that the identities chosen by the sender and receiver can be checked simultaneously without revealing any information other than whether the match is successful or not.

– Second, this variant of two-level IBE is built from Okamoto and Takashima's dual pairing vector spaces [25] and its security reductions rely on Waters's dual system encryption [32]. During the security proof process, we draw on the idea of delegation functionality in Okamoto and Takashima's hierarchical inner-product encryption [26] and slightly extended the dual system methodology to fit our IB-ME scheme. We rely on an information theoretic argument instead of computational arguments in the final step of the proof. This is the first work to build identity-based matchmaking encryption by combining dual pairing vector spaces and dual system encryption under the standard assumptions.

1.2 Technical Overview

To achieve the above results, we propose a new technique for designing IB-ME schemes, its construction is straightforward and does not rely on other crypto tools. More concretely, we present a variant of two-level IBE with anonymity and unforgeability that satisfies the same functionality of IB-ME. Moreover, its security properties cleverly meet the two requirements of IB-ME (privacy and authenticity). An IB-ME scheme consists of five algorithms, namely Setup that generates the master public key mpk and master secret key msk, SKGen that generates the encryption key ek_σ using the sender's identity σ, RKGen that generates the decryption key dk_ρ using the receiver's identity ρ, Enc that encrypts the message using ek_σ and a target identity rcv, and Dec that decrypts the ciphertext using dk_ρ and a target identity snd. Decryption can be successful if and only if the attributes of the sender and receiver satisfy the target identity respectively, i.e. $\sigma = \mathsf{snd} \wedge \rho = \mathsf{rcv}$. At the same time, an IB-ME should satisfy two main security properties: $\mathsf{privacy}$ and $\mathsf{authenticity}$ [3].

Informally, in this variant of two-level IBE, the algorithms RKGen and Enc associated by identities ρ and rcv are the first level, while the second level consists of the algorithms SKGen and Dec associated by identities σ and snd. The

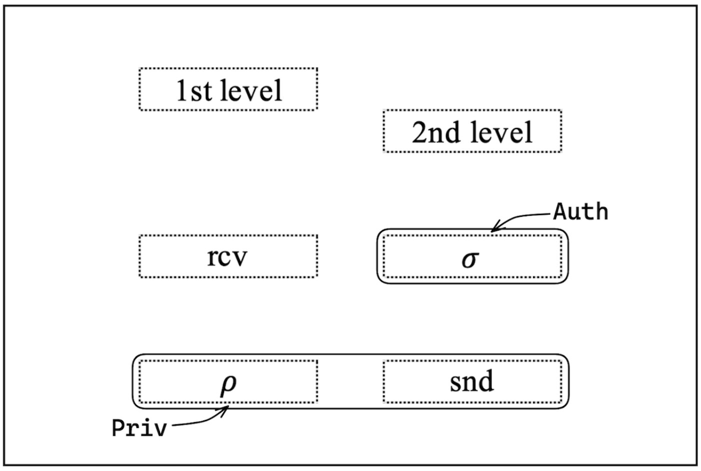

Fig. 1. Security requirements of IB-ME

privacy property of IB-ME relies on the anonymity of this 2-level IBE, while the authenticity property is corresponding to the unforgeability in the 2nd level as all shown in Fig. 1. Decryption can only be done when both levels are matched successfully. Different from IBE, a part of the two keys ek_σ, dk_ρ need to be generated from msk, and each identity-related parameter needs to be generated separately. More concretely, it can be observed that in game $\mathbf{G}^{\mathsf{ib\text{-}priv}}_{\Pi,\mathsf{A}}(\lambda)$ defining $\mathsf{privacy}$, the adversary outputs two sets of challenge pairs $(m_0, \mathsf{rcv}_0, \sigma_0)$ and $(m_1, \mathsf{rcv}_1, \sigma_1)$ after querying oracles, and then outputs b' for guessing. In game $\mathbf{G}^{\mathsf{ib\text{-}auth}}_{\Pi,\mathsf{A}}(\lambda)$ defining $\mathsf{authenticity}$, the adversary is actually similar to being unable to forge a ciphertext ct about the message m. The former can be considered as a property of anonymity, while the latter generates an unforgeable signature. Therefore, a two-level anonymous IBE (a signature scheme can be derived from the same IBE) can be used to instantiate this construction and can achieve the security requirements simultaneously.

Our first thought was to use Lewko-Waters composite order IBE scheme [21] for the advantage of its efficiency and shorter parameters, but in view of its difficulty in extending to high-dimensional spaces, we finally decided to choose the prime-order group IBE scheme based on DPVS as the basis of our construction. Meanwhile, since a part of the decryption key dk_ρ needs to be generated from msk, we borrow some ideas from constructing hierarchical inner-product predicate encryption. Specifically, Chen's anonymous IBE [13] and Okamoto and Takashima's HIPE [26] together form the blueprint of this variant of two-level IBE. Thus the message and all identities can be hidden in the high-dimensional basis vectors of the linear subspace. As for security, the privacy property is consistent with proving the full security and anonymity of the 1st level IBE through the dual system encryption methodology. When proving the authenticity property which is similar to the unforgeability of signatures, we make a transformation from IB-ME to IBE and land it on the security of this IBE system. The rest of the proof is similar to that in [13,19].

1.3 Related Work

The idea of using some unique information about the identity of a user as his public encryption key was conceived by Shamir [30] in 1984 and is known as Identity-Based Encryption (IBE). In an identity-based encryption system, a sender who has access to the public parameters can encrypt a message using the target receiver's identity, and the ciphertext can only be decrypted by a receiver who satisfies this identity. 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 [7,15,17], to more recent constructions in the standard model [5,6,9,2,14].

In order to overcome the limitations of partitioning [31], Waters presented a new methodology dubbed dual system encryption [32] for obtaining fully secure IBE and HIBE systems from simple assumptions. It was further developed in several subsequent works [21,22,23,24] by Lewko and Waters to enhance the security and the efficiency. Most of these works have used composite order groups as a convenient setting for instantiating the dual system, but with the introduction of dual pairing vector spaces (DPVS) by Okamoto and Takashima [25,26,28], which is a brand new technique based on bilinear pairing groups of prime order, some practical and flexible works emerged. A number of functional encryption schemes [20,27,29,13] that intelligently combine dual system encryption and DPVS have a better performance. Then Lewko et al. successfully explored a general framework [19] based on *pair encoding* [4] summarized by Attrapadung for converting composite order pairing-based cryptosystems into prime order settings and obtained fully secure IBE and HIBE schemes. Chen et al. presented a modular framework [10] based on *predicate encodings* [33] proposed by Wee for the design of efficient adaptively secure attribute-based encryption (ABE) schemes for a large class of predicates under the standard k-Lin assumption in prime-order groups and obtained concrete efficiency improvements for several ABE schemes.

The notion of IB-ME proposed by Ateniese et al. in [3] is a generalization of IBE where the sender and the receiver can both specify a target identity. Following their works, Xu et al. [34] proposed matchmaking attribute-based encryption by extending the IB-ME scheme, and apply it to construct a secure fine-grained bilateral access control data sharing system in cloud-fog computing. They also introduced a new cryptographic tool called lightweight matchmaking encryption [35] and constructed a secure cloud-fog IoT data sharing system with bilateral access control.

Organization : The rest of this paper is organized as follows: Section 2 introduces the necessary preliminaries on dual pairing vector spaces and SXDH assumption. We give the definitions of IBE and recall the syntax and security of IB-ME in Section 3. We detail our scheme and prove its security in Section 4. A brief conclusion and future works are in Section 5.

2 Preliminaries

In what follows, we first introduce some notations used in this work. Then we give a few preliminaries related to groups with efficiently computable bilinear maps and define the Symmetric External Diffie-Hellman assumption.

Notation: If S is a finite set, then $r \overset{R}{\leftarrow} \mathsf{S}$ denotes sampling r uniformly at random from S. If f is an algorithm or function, then $y \leftarrow f(x)$ denotes the output of this algorithm with x as input. $y := x$ denotes that y is defined or substituted by x. Unless otherwise specified, algorithms in this work are randomized and PPT stands for probabilistic polynomial time. We use lowercase letters (e.g., r, s, t) to denote elements in vectors or matrices, bold lowercase letters (e.g., $\mathbf{b_1}, \mathbf{d_2}, \mathbf{f_3^*}$) to denote vectors and bold uppercase letters (e.g., $\mathbf{A}$) to denote matrices. We say a function $\varepsilon(\lambda)$ is *negligible* in λ, if $\varepsilon(\lambda) = o(1/\lambda^c)$ for every $c \in \mathbb{Z}$, and we write $\mathsf{negl}(\lambda)$ to denote a negligible function in λ.

2.1 Dual Pairing Vector Spaces

Our constructions are based on dual pairing vector spaces proposed by Okamoto and Takashima [25,26]. In this work, we concentrate on the asymmetric version [27]. We only briefly describe how to generate random dual orthonormal bases. See [25,26,27] for a full definition of dual pairing vector spaces.

Definition 1 (Asymmetric bilinear pairing groups). *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 $e : G_1 \times G_2 \rightarrow G_T$ 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 and G_2, we will also consider "vectors" of group elements. For $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{Z}_q^n$ and $g_\beta \in G_\beta$, we write $g_\beta^{\mathbf{v}}$ to denote an n-tuple of elements of G_β for $\beta = 1, 2$:

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

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

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

Then we define

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

Here, the dot product is taken modulo q.

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

$$\mathbf{b}_j \cdot \mathbf{b}_k^* = 0 \, (\mathsf{mod}\ q)$$

whenever $j \neq k$, and

$$\mathbf{b}_j \cdot \mathbf{b}_j^* = \psi \, (\mathsf{mod}\ q)$$

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

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

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

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

More generally, we can sample multiple tuple of "dual orthonormal" bases. Namely, for fixed (constant) dimension $n_1, \ldots, n_d$, we will choose d tuples of two random bases $\mathbb{B}_i := (\mathbf{b}_{1,i}, \ldots, \mathbf{b}_{n_i,i})$ and $\mathbb{B}_i^* := (\mathbf{b}_{1,i}^*, \ldots, \mathbf{b}_{n_i,i}^*)$ of $\mathbb{Z}_q^{n_i}$, subject to the constraint that they are "dual orthonormal", meaning that

$$\mathbf{b}_{j,i} \cdot \mathbf{b}_{k,i}^* = 0 \, (\mathsf{mod}\ q)$$

whenever $j \neq k$, and

$$\mathbf{b}_{j,i} \cdot \mathbf{b}_{j,i}^* = \psi \, (\mathsf{mod}\ q)$$

for all j, where ψ is a random element of $\mathbb{Z}_q$. We denote such algorithm as $\mathsf{Dual}(\mathbb{Z}_q^{n_1}, \ldots, \mathbb{Z}_q^{n_d})$.

2.2 SXDH Assumptions

Definition 2 (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}),

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

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 Definition 2 with the roles of G_1 and G_2 reversed. We say that:

Definition 3. *The Symmetric External Diffie-Hellman assumption holds if DDH problems are intractable in both G_1 and G_2.*

2.3 Subspace Assumptions via SXDH

In this subsection, we present subspace assumptions derived from the SXDH assumption. We will rely on these assumptions later to instantiate our encryption schemes. These are analogues of the DLIN-based Subspace assumptions given in [12,19,27].

Definition 4 (DS1: Decisional Subspace Assumption in G_1). *Given a group generator $\mathcal{G}(\cdot)$, define the following distribution:*

$$\begin{aligned}
&\mathbb{G} := (q, G_1, G_2, G_T, g_1, g_2, e) \xleftarrow{R} \mathcal{G}(1^\lambda),\\
&(\mathbb{B}, \mathbb{B}^*) \xleftarrow{R} \mathsf{Dual}(\mathbb{Z}_q^N); \tau_1, \tau_2, \mu_1, \mu_2 \xleftarrow{R} \mathbb{Z}_q,\\
&U_1 := g_2^{\mu_1 \mathbf{b}_1^* + \mu_2 \mathbf{b}_{K+1}^*}, \ldots, U_K := g_2^{\mu_1 \mathbf{b}_K^* + \mu_2 \mathbf{b}_{2K}^*},\\
&V_1 := g_1^{\tau_1 \mathbf{b}_1}, \ldots, V_K := g_1^{\tau_1 \mathbf{b}_K},\\
&W_1 := g_1^{\tau_1 \mathbf{b}_1 + \tau_2 \mathbf{b}_{K+1}}, \ldots, W_K := g_1^{\tau_1 \mathbf{b}_K + \tau_2 \mathbf{b}_{2K}},
\end{aligned}$$

$$D := (\mathbb{G}; g_2^{\mathbf{b}_1^*}, \ldots, g_2^{\mathbf{b}_K^*}, g_2^{\mathbf{b}_{2K+1}^*}, \ldots, g_2^{\mathbf{b}_N^*}, g_1^{\mathbf{b}_1}, \ldots, g_1^{\mathbf{b}_N}, U_1, \ldots, U_K, \mu_2)$$

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

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

is negligible in the security parameter λ.

For our construction, we only require the assumption for $K = 4$ and $N = 8$. Furthermore, we do not need to provide μ_2 to the distinguisher. Informally, this means that, given $\tau_1, \tau_2, \mu_1, \mu_2 \xleftarrow{R} \mathbb{Z}_q$ and

$$U_1 = g_2^{\mu_1 \mathbf{b}_1^* + \mu_2 \mathbf{b}_5^*}, U_2 = g_2^{\mu_1 \mathbf{b}_2^* + \mu_2 \mathbf{b}_6^*}, U_3 = g_2^{\mu_1 \mathbf{b}_3^* + \mu_2 \mathbf{b}_7^*}, U_4 = g_2^{\mu_1 \mathbf{b}_4^* + \mu_2 \mathbf{b}_8^*},$$

the distributions (V_1, V_2, V_3, V_4) and (W_1, W_2, W_3, W_4) are computationally indistinguishable, where:

$$\begin{aligned}
&V_1 = g_1^{\tau_1 \mathbf{b}_1}, V_2 = g_1^{\tau_1 \mathbf{b}_2}, V_3 = g_1^{\tau_1 \mathbf{b}_3}, V_4 = g_1^{\tau_1 \mathbf{b}_4};\\
&W_1 = g_1^{\tau_1 \mathbf{b}_1 + \tau_2 \mathbf{b}_5}, W_2 = g_1^{\tau_1 \mathbf{b}_2 + \tau_2 \mathbf{b}_6}, W_3 = g_1^{\tau_1 \mathbf{b}_3 + \tau_2 \mathbf{b}_7}, W_4 = g_1^{\tau_1 \mathbf{b}_4 + \tau_2 \mathbf{b}_8}.
\end{aligned}$$

Lemma 1. *If the DDH assumption in G_1 holds, then the Subspace assumption in G_1 stated in Definition 4 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. Detailed proofs can be found in [12].

The dual of the Subspace assumption in G_1 is Subspace assumption in G_2 (denoted as DS2), which is identical to Definition 4 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.

2.4 Statistical Indistinguishability Lemma

We require the following lemma for our security proofs, which is derived from [27].

Lemma 2. *For $p \in \mathbb{Z}_q$, let $C_p := \{(\mathbf{x}, \mathbf{v}) | \mathbf{x} \cdot \mathbf{v} = p, \mathbf{0} \neq \mathbf{x}, \mathbf{0} \neq \mathbf{v} \in \mathbb{Z}_q^n\}$. For all $(\mathbf{x}, \mathbf{v}) \in C_p$, for all $(\mathbf{z}, \mathbf{w}) \in C_p$, and $\mathbf{A} \xleftarrow{R} \mathbb{Z}_q^{n \times n}$ ($\mathbf{A}$ is invertible with overwhelming probability),*

$$\mathsf{Pr}[\mathbf{x}\mathbf{A}^\top = \mathbf{z} \ \wedge \ \mathbf{v}\mathbf{A}^{-1} = \mathbf{w}] = \frac{1}{\# C_p}.$$

3 Identity-Based Matchmaking Encryption

In what follows, we first recall the definitions of identity-based encryption and signatures. Then we introduce the definition of identity-based matchmaking encryption presented in [3].

3.1 Identity-Based Encryption

In the IBE setting, a functionality $\hat{F}$ is defined over a key space and an index space using sets of identities. The key space $\mathcal{K}$ and index space $\mathcal{I}$ for IBE then corresponds to all identities id. Here

$$\hat{F}(\mathsf{id}, (\mathsf{id}', m)) := \begin{cases} m & \text{if } \mathsf{id}' = \mathsf{id} \\ \perp & \text{otherwise.} \end{cases}$$

An Identity-Based Encryption [7] scheme consists of following four algorithms: Setup, KeyGen, Enc, and Dec.

- $\mathsf{Setup}(\lambda) \to (pp, mk)$: The setup algorithm takes in the security parameter λ, and outputs the public parameters pp, and the master key mk.
- $\mathsf{KeyGen}(pp, mk, \mathsf{id}) \to sk_{\mathsf{id}}$: The key generation algorithm takes in the public parameters pp, the master key mk, an identity id and produces a secret key sk_{id} for that identity.
- $\mathsf{Enc}(pp, \mathsf{id}, m) \to ct_{\mathsf{id}}$: The encryption algorithm takes in the public parameters pp, an identity id, a message m and outputs a ciphertext ct_{id} encrypted under that identity.
- $\mathsf{Dec}(pp, sk_{\mathsf{id}}, ct_{\mathsf{id}}) \to m$: 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.

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 adversider $\mathcal{A}$.

- 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 adversary $\mathcal{A}$ adaptively requests key for identities id, and is provided with corresponding secret key sk_{id}, which the challenger $\mathcal{B}$ generates by running the key generation algorithm.
- $\mathsf{Challenge}$: The adversary $\mathcal{A}$ gives $\mathcal{B}$ two challenge pairs (m_0, id_0^*) and (m_1, id_1^*). The challenge identities must not have been queried in $\mathsf{Phase\ 1}$. The challenger $\mathcal{B}$ sets $\beta \in \{0, 1\}$ randomly, and encrypts m_β under id_β^* by running the encryption algorithm. It send the ciphertext to the adversary $\mathcal{A}$.
- $\mathsf{Phase\ 2}$: This is the same as $\mathsf{Phase\ 1}$ with the added restriction a secret key for $\mathsf{id}_0^*, \mathsf{id}_1^*$ cannot be requested.
- Guess: The adversary $\mathcal{A}$ must output a guess β' for β.

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

Definition 5. *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 1: The security notion of non-anonymous IBE is defined as above with restriction that $\mathsf{id}_0^* = \mathsf{id}_1^*$.

3.2 Signature Schemes

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

- $\mathsf{KeyGen}(1^\lambda)$: The key generation algorithm takes in the security parameter 1^λ, and outputs the public key pk, and the secret key sk.
- $\mathsf{Sign}(sk, m)$: The signing algorithm takes in the secret key sk and a message m, and produces a signature σ for this message.
- $\mathsf{Verify}(pk, \sigma, m)$: 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 [18], which is defined using the following game between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

- Setup : The challenger $\mathcal{C}$ runs the key generation algorithm to generate pk and sk. It gives pk to the adversary $\mathcal{A}$.
- Query : 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 (σ, m).

The advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Sig}}(\lambda)$ 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) $\mathsf{Verify}(pk, \sigma, m)$ outputs `valid`.

Definition 6. *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 1^λ. We note that the security of the signature scheme can follow from the security of IBE scheme by applying Naor's transform [7,8].

3.3 Syntax of IB-ME

In IB-ME, attributes and policies are treated as binary strings. We denote with rcv and snd the target identities or policies chosed by the sender and the receiver, respectively. We say that a match (resp. mismatch) occurs when $\sigma = \mathsf{snd}$ and $\rho = \mathsf{rcv}$ (resp. $\sigma \neq \mathsf{snd}$ or $\rho \neq \mathsf{rcv}$). The receiver can choose the target identity snd on the fly. More formally, an IB-ME scheme is composed of the following five polynomial-time algorithms:

- $\mathsf{Setup}(1^\lambda) \rightarrow (mpk, msk)$: Upon input the security parameter 1^λ, the randomized setup algorithm outputs the master public key mpk and the master secret key msk.
- $\mathsf{SKGen}(mpk, msk, \sigma) \rightarrow ek_\sigma$: Upon input the master secret key msk and the identity σ, the randomized sender-key generator outputs an encryption key ek_σ for σ.
- $\mathsf{RKGen}(mpk, msk, \rho) \rightarrow dk_\rho$: Upon input the master secret key msk and the identity ρ, the randomized receiver-key generator outputs a decryption key dk_ρ for ρ.
- $\mathsf{Enc}(mpk, ek_\sigma, \mathsf{rcv}, m) \rightarrow ct$: Upon input the encryption key ek_σ for identity σ, a target identity rcv and a message $m \in \mathcal{M}$, the randomized encryption algorithm produces a ciphertext ct linked to both σ and rcv.
- $\mathsf{Dec}(mpk, dk_\rho, \mathsf{snd}, ct) \rightarrow m$: Upon input the decryption key dk_ρ for identity ρ, a target identity snd and a ciphertext ct, the deterministic decryption algorithm outputs either a message m or $\perp$.

Correctness. Correctness of IB-ME simply says that in case of a match the receiver obtains the plaintext.

Definition 7 (Correctness of IB-ME). *An IB-ME scheme* $\mathit{\Pi} =(\mathsf{Setup}, \mathsf{SKGen}, \mathsf{RKGen}, \mathsf{Enc}, \mathsf{Dec})$ *is correct if* $\forall \lambda \in \mathbb{N}$, $\forall (mpk, msk)$ *output by* $\mathsf{Setup}(1^\lambda)$, $\forall m \in \mathcal{M}$, $\forall \sigma, \rho, \mathsf{rcv}, \mathsf{snd} \in \{0,1\}^*$ *such that* $\sigma = \mathsf{snd}$ *and* $\rho = \mathsf{rcv}$*:*

$$\mathsf{Pr}[\mathsf{Dec}(dk_\rho, \mathsf{snd}, \mathsf{Enc}(ek_\sigma, \mathsf{rcv}, m)) = m] \geq 1 - \mathsf{negl}(\lambda),$$

where $ek_\sigma \xleftarrow{R} \mathsf{SKGen}(msk, \sigma)$ *and* $dk_\rho \xleftarrow{R} \mathsf{RKGen}(msk, \rho)$.

3.4 Security of IB-ME

We now define $\mathsf{privacy}$ and $\mathsf{authenticity}$ of IB-ME. Recall that privacy captures secrecy of the sender's inputs $(\sigma, \mathsf{rcv}, m)$. This is formalized by asking the adversary to distinguish between $\mathsf{Enc}(ek_{\sigma_0}, \mathsf{rcv}_0, m_0)$ and $\mathsf{Enc}(ek_{\sigma_1}, \mathsf{rcv}_1, m_1)$ where $(m_0, m_1, \sigma_0, \sigma_1, \mathsf{rcv}_0, \mathsf{rcv}_1)$ are chosen by the attacker. The definition of authenticity intuitively says that an adversary cannot compute a valid ciphertext under the identity σ, if it does not hold the corresponding encryption key ek_σ produced by the challenger.

```
$\mathbf{G}^{\mathsf{ib\text{-}priv}}_{\Pi,\mathsf{A}}(\lambda)$
$(\mathsf{mpk}, \mathsf{msk}) \xleftarrow{R} \mathsf{Setup}(1^\lambda)$
$(m_0, m_1, \mathsf{rcv}_0, \mathsf{rcv}_1, \sigma_0, \sigma_1, st) \xleftarrow{R} \mathsf{A}_1^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, \mathsf{mpk})$
$b \xleftarrow{R} \{0,1\}$
$ek_{\sigma_b} \xleftarrow{R} \mathsf{SKGen}(\mathsf{msk}, \sigma_b)$
$ct \xleftarrow{R} \mathsf{Enc}(ek_{\sigma_b}, \mathsf{rcv}_\mathsf{b}, m_b)$
$b' \xleftarrow{R} \mathsf{A}_2^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, ct, st)$
If$(b' = b)$ return 1
Else return 0
```

```
$\mathbf{G}^{\mathsf{ib\text{-}auth}}_{\Pi,\mathsf{A}}(\lambda)$
$(\mathsf{mpk}, \mathsf{msk}) \xleftarrow{R} \mathsf{Setup}(1^\lambda)$
$(ct, \rho, \mathsf{snd}) \xleftarrow{R} \mathsf{A}^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, \mathsf{mpk})$
$dk_\rho \xleftarrow{R} \mathsf{RKGen}(\mathsf{msk}, \rho)$
$m = \mathsf{Dec}(dk_\rho, \mathsf{snd}, ct)$
If $\forall \sigma \in \mathcal{Q}_{\mathsf{O}_1} : (\sigma \neq \mathsf{snd}) \wedge (m \neq \perp)$
    return 1
Else return 0
```

Fig. 2. Games defining privacy and authenticity security of IB-ME. Oracles $\mathsf{O}_1, \mathsf{O}_2$ are implemented by $\mathsf{SKGen}(\mathsf{msk}, \cdot), \mathsf{RKGen}(\mathsf{msk}, \cdot)$.

Definition 8 (Privacy of IB-ME). *We say that an IB-ME Π satisfies privacy if for all valid PPT adversaries $\mathcal{A} = (\mathsf{A}_1, \mathsf{A}_2)$:*

$$\left| \Pr[\mathbf{G}^{\mathsf{ib\text{-}priv}}_{\Pi,\mathsf{A}}(\lambda) = 1] - \frac{1}{2} \right| \leq \mathsf{negl}(\lambda)$$

where game $\mathbf{G}^{\mathsf{ib\text{-}priv}}_{\Pi,\mathsf{A}}(\lambda)$ is depicted in Fig.2. Adversary $\mathcal{A}$ is called valid if $\forall \rho \in \mathcal{Q}_{\mathsf{O}_2}$ it satisfies the following invariant:

$$(\textbf{Mismatch condition}) : \rho \neq \mathsf{rcv}_0 \wedge \rho \neq \mathsf{rcv}_1.$$

Definition 9 (Authenticity of IB-ME). *We say that an IB-ME Π satisfies authenticity if for all valid PPT adversaries $\mathcal{A}$:*

$$\Pr[\mathbf{G}^{\mathsf{ib\text{-}auth}}_{\Pi,\mathsf{A}}(\lambda) = 1] \leq \mathsf{negl}(\lambda)$$

where game $\mathbf{G}^{\mathsf{ib\text{-}auth}}_{\Pi,\mathsf{A}}(\lambda)$ is depicted in Fig.2.

Definition 10 (Secure IB-ME). *We say that an IB-ME Π is secure if it satisfies privacy (Def.8) and authenticity (Def.9).*

4 The Proposed IB-ME Construction

We are now ready to give the concrete construction of our IB-ME scheme.

4.1 Construction

- $\mathsf{Setup}(1^\lambda) \to (mpk, msk)$: This algorithm takes in the security parameter 1^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 $(\mathbb{D}, \mathbb{D}^*) \xleftarrow{R} \mathsf{Dual}(\mathbb{Z}_q^8)$. Let $\mathbf{d_1}, ..., \mathbf{d_8}$ denote the elements of $\mathbb{D}$ and $\mathbf{d_1^*}, ..., \mathbf{d_8^*}$ denote the elements of $\mathbb{D}^*$. Let $g_T := e(g_1, g_2)^{\mathbf{d_1} \cdot \mathbf{d_1^*}}$. It also picks $\alpha, \eta \xleftarrow{R} \mathbb{Z}_q$ and outputs the master public key as
$$mpk := \{\mathbb{G}; g_T^\alpha, g_T^\eta, g_1^{\mathbf{d_1}}, g_1^{\mathbf{d_2}}\},$$
and the master secret key
$$msk := \{\alpha, \eta, g_1^{\mathbf{d_3}}, g_1^{\mathbf{d_4}}, g_2^{\mathbf{d_1^*}}, g_2^{\mathbf{d_2^*}}, g_2^{\mathbf{d_3^*}}, g_2^{\mathbf{d_4^*}}\}.$$
- $\mathsf{SKGen}(mpk, msk, \sigma) \to ek_\sigma$: This algorithm picks $r \xleftarrow{R} \mathbb{Z}_q$. The encryption key is computed as
$$ek_\sigma := g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}.$$
- $\mathsf{RKGen}(mpk, msk, \rho) \to dk_\rho$: This algorithm picks $s, s_1, s_2 \xleftarrow{R} \mathbb{Z}_q$. The decryption key is computed as
$$dk_\rho := \{k_1 = g_2^{\alpha \mathbf{d_1^*} + s_1(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s\mathbf{d_3^*}}, k_2 = g_2^{s_2(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s\mathbf{d_4^*}}, k_3 = (g_T^\eta)^s\}.$$
- $\mathsf{Enc}(mpk, ek_\sigma, \mathsf{rcv}, m) \to ct$: This algorithm picks $z \xleftarrow{R} \mathbb{Z}_q$ and forms the ciphertext as
$$ct := \{\mathsf{C} = m \cdot (g_T^\alpha)^z, \mathsf{C_0} = ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathsf{rcv}\mathbf{d_2})}\}.$$
- $\mathsf{Dec}(mpk, dk_\rho, \mathsf{snd}, ct) \to m$: This algorithm computes the message as
$$m := \frac{\mathsf{C}}{e(\mathsf{C_0}, k_1 \cdot k_2^{\mathsf{snd}}) \cdot k_3^{-1}}.$$

Correctness: Correctness follows when $\mathsf{snd} = \sigma$ and $\mathsf{rcv} = \rho$:

$$\begin{aligned}
&e(\mathsf{C_0}, k_1 \cdot k_2^{\mathsf{snd}}) \\
=&e(g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4}) + z(\mathbf{d_1} + \mathsf{rcv}\mathbf{d_2})}, g_2^{\alpha \mathbf{d_1^*} + (s_1 + s_2 \cdot \mathsf{snd})(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s(\mathbf{d_3^*} + \mathsf{snd}\mathbf{d_4^*})}) \\
=&e(g_1, g_2)^{\eta s \mathbf{d_3} \cdot \mathbf{d_3^*} + rs(\sigma \mathbf{d_3} \cdot \mathbf{d_3^*} - \mathsf{snd}\mathbf{d_4} \cdot \mathbf{d_4^*}) + \alpha z \mathbf{d_1} \cdot \mathbf{d_1^*} + z(s_1 + s_2 \cdot \mathsf{snd})(\rho \mathbf{d_1} \cdot \mathbf{d_1^*} - \mathsf{rcv}\mathbf{d_2} \cdot \mathbf{d_2^*})} \\
=&e(g_1, g_2)^{\eta s \mathbf{d_3} \cdot \mathbf{d_3^*} + \alpha z \mathbf{d_1} \cdot \mathbf{d_1^*}} = (g_T)^{\eta s + \alpha z}
\end{aligned}$$

$$\frac{\mathsf{C}}{e(\mathsf{C_0}, k_1 \cdot k_2^{\mathsf{snd}}) \cdot k_3^{-1}} = \frac{m \cdot (g_T^\alpha)^z}{(g_T)^{\eta s + \alpha z} \cdot g_T^{-\eta s}} = m$$

4.2 Security Analysis

As for security, it can be proved that our proposed IB-ME scheme is secure (Def. 10) according to the Theorem 1 and Theorem 2, namely satisfies $\mathsf{privacy}$ (Def. 8) and $\mathsf{authenticity}$ (Def. 9) simultaneously.

Theorem 1. *The proposed IB-ME scheme satisfies privacy under the Symmetric External Diffie-Hellman assumption. More precisely, for any PPT adversary $\mathcal{A}$ breaks the privacy property of our IB-ME scheme, there exist probabilistic algorithms $\mathcal{B}_0, \mathcal{B}_{1,1}, \mathcal{B}_{1,2}, \ldots, \mathcal{B}_{\nu,1}, \mathcal{B}_{\nu,2}$ whose running times are essentially the same as that of $\mathcal{A}$, such that*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IB\text{-}ME}}(\lambda) \leq \mathsf{Adv}_{\mathcal{B}_0}^{\mathsf{DDH1}}(\lambda) + \sum_{\kappa=1}^{\nu} \Big(\mathsf{Adv}_{\mathcal{B}_{\kappa,1}}^{\mathsf{DDH2}}(\lambda) + \mathsf{Adv}_{\mathcal{B}_{\kappa,2}}^{\mathsf{DDH2}}(\lambda)\Big) + (12\nu + 3)/q$$

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

Proof Outline: There are many similarities between the proof of our scheme and the anonymous IBE scheme in [12]. We will follow a similar strategy of proving fully secure anonymous IBE, adopting the dual system encryption methodology by Waters [32] to prove that our IB-ME satisfies privacy under the SXDH assumption. The hardest part of the security proof is how to prove the negligible gap between two different forms of dk_ρ, especially when it is composed of three different keys k_1, k_2 and k_3. In order to solve this problem, apart from the concepts of *semi-functional ciphertexts* and *semi-functional keys* in our proof, we introduce the concept of *inter-semi-functional secret key* and provide algorithms that generate them. More precisely, *inter-semi-functional key* means that k_1 is semi-functional and k_2 is normal, while *semi-functional key* means that both k_1 and k_2 are semi-functional, and k_3 always remains the same. We note that these algorithms are only provided in a sequence of security games for the proof, and are not part of the IB-ME scheme. In particular, they do not need to be efficiently computable from the master public key and the master secret key. Meanwhile, another ν games are added into the proof, and for κ from 1 to ν, all the decryption keys will be converted into semi-functional keys step by step according to the sequence of changing normal key to *inter*-semi-functional key first in $\mathsf{Game}_{\kappa,1}$ and then changing it to semi-functional key in $\mathsf{Game}_{\kappa,2}$. In other words, we consider k_1 and k_2 in dk_ρ as two independent keys and generate their semi-functional keys in the **KeyGenSF** algorithm respectively. We first require that the challenger can simulate the two different forms of k_1, and then require it can simulate the two different forms of k_2 with the adversary. Then, we adopt the same procedure as in the security model definition, treating the output of SKGen algorithm as a part of the input to Enc algorithm, from which the corresponding semi-functional ciphertext is generated.

KeyGenSF: The algorithm picks $s, s_1, s_2, \{s_{i,1}\}_{i=5,\ldots,8} \xleftarrow{R} \mathbb{Z}_q$ and forms the inter-semi-functional secret key as

$$\begin{aligned}\mathsf{dk}_{\rho}^{(\mathsf{inter\text{-}SF})} := \{\ k_1 = g_2^{\alpha \mathbf{d}_1^* + s_1(\rho \mathbf{d}_1^* - \mathbf{d}_2^*) + s\mathbf{d}_{\mathbf{3}}^* + [s_{5,1}\mathbf{d}_5^* + s_{6,1}\mathbf{d}_6^* + s_{7,1}\mathbf{d}_{\mathbf{7}}^*]},\\ k_2 = g_2^{s_2(\rho \mathbf{d}_1^* - \mathbf{d}_2^*) + s\mathbf{d}_{\mathbf{4}}^*},\ k_3 = (g_T^{\eta})^s\}; \qquad (1)\end{aligned}$$

The algorithm picks $s, s_1, s_2, \{s_{i,j}\}_{i=5,\ldots,8;j=1,2} \xleftarrow{R} \mathbb{Z}_q$ and forms the semi-functional secret key as

$$\begin{aligned}\mathsf{dk}_{\rho}^{(\mathsf{SF})} := \{\ k_1 = g_2^{\alpha \mathbf{d}_1^* + s_1(\rho \mathbf{d}_1^* - \mathbf{d}_2^*) + s\mathbf{d}_{\mathbf{3}}^* + [s_{5,1}\mathbf{d}_5^* + s_{6,1}\mathbf{d}_6^* + s_{7,1}\mathbf{d}_{\mathbf{7}}^*]},\\ k_2 = g_2^{s_2(\rho \mathbf{d}_1^* - \mathbf{d}_2^*) + s\mathbf{d}_{\mathbf{4}}^* + [s_{5,2}\mathbf{d}_5^* + s_{6,2}\mathbf{d}_6^* + s_{8,2}\mathbf{d}_{\mathbf{8}}^*]},\ k_3 = (g_T^{\eta})^s\}. \qquad (2)\end{aligned}$$

Hereafter we will ignore k_3 since it is always correctly generated.

EncryptSF: The algorithm picks $z, r, r_5, r_6, r_7, r_8 \xleftarrow{R} \mathbb{Z}_q$ and forms a semi-functional ciphertext as

$$ek_{\sigma} := g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$$

$$\begin{aligned}\mathsf{CT}_{ek_{\sigma},\mathsf{rcv}}^{(\mathsf{SF})} := \{\mathsf{C} : = m \cdot (g_T^{\alpha})^z, \mathsf{C}_0 := ek_{\sigma} \cdot g_1^{z(\mathbf{d_1} + \mathsf{rcv}\mathbf{d_2}) + [r_5\mathbf{d_5} + r_6\mathbf{d_6} + r_7\mathbf{d_7} + r_8\mathbf{d_8}]}\\ = \ g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4}) + z(\mathbf{d_1} + \mathsf{rcv}\mathbf{d_2}) + [r_5\mathbf{d_5} + r_6\mathbf{d_6} + r_7\mathbf{d_7} + r_8\mathbf{d_8}]}\}. \qquad (3)\end{aligned}$$

Hereafter we will ignore C since it is always correctly generated. We observe that if one applies the decryption procedure with a (inter) semi-functional key and a normal ciphertext, decryption will succeed because $(\mathbf{d}_5^*, \mathbf{d}_6^*, \mathbf{d}_7^*, \mathbf{d}_8^*)$ are orthogonal to all of the vectors in exponent of C_0, and hence have no effect on decryption. Similarly, decryption of a semi-functional ciphertext by a normal key will also succeed because $(\mathbf{d}_5, \mathbf{d}_6, \mathbf{d}_7, \mathbf{d}_8)$ 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 decryption procedure $e(\mathsf{C}_0, k_1 \cdot k_2^{\mathsf{snd}}) \cdot k_3^{-1}$ will have an additional term, namely

$$e(g_1, g_2)^{r_5(s_{5,1} + \mathsf{snd} \cdot s_{5,2})\mathbf{d_5} \cdot \mathbf{d}_{\mathbf{5}}^* + r_6(s_{6,1} + \mathsf{snd} \cdot s_{6,2})\mathbf{d_6} \cdot \mathbf{d}_{\mathbf{6}}^* + r_7 s_{7,1}\mathbf{d_7} \cdot \mathbf{d}_{\mathbf{7}}^* + r_8 \cdot \mathsf{snd} \cdot s_{8,2}\mathbf{d_8} \cdot \mathbf{d}_{\mathbf{8}}^*}$$

$$= g_T^{(r_5 s_{5,1} + r_6 s_{6,1} + r_7 s_{7,1}) + \mathsf{snd}(r_5 s_{5,2} + r_6 s_{6,2} + r_8 s_{8,2})}.$$

Decryption will then fail unless $r_5 s_{5,1} + r_6 s_{6,1} + r_7 s_{7,1} \equiv 0 \pmod{q}$ and $r_5 s_{5,2} + r_6 s_{6,2} + r_8 s_{8,2} \equiv 0 \pmod{q}$. If this modular equation holds, we say that this key and ciphertext pair is *nominally semi-functional.*

For a probabilistic polynomial-time adversary $\mathcal{A}$ which makes ν key queries $\mathsf{rcv}_1, \ldots, \mathsf{rcv}_{\nu}$, our proof of security consists of the following sequence of games between $\mathcal{A}$ and a challenger $\mathcal{B}$.

- $\mathsf{Game}_{\mathsf{Real}}$: is the real security game.
- Game_0: is the same as $\mathsf{Game}_{\mathsf{Real}}$ except that the challenge ciphertext is semi-functional.

- $\mathsf{Game}_{\kappa,1}$: for κ from 1 to ν, $\mathsf{Game}_{\kappa,1}$ is the same as Game_0 except that the first κ-1 keys are semi-functional, the κ-th key is inter-semi-functional and the remaining keys are normal.
- $\mathsf{Game}_{\kappa,2}$: for κ from 1 to ν, $\mathsf{Game}_{\kappa,2}$ is the same as Game_0 except that the first κ keys are semi-functional and the remaining keys are normal.
- $\mathsf{Game}_{\mathsf{Final}}$: is the same as $\mathsf{Game}_{\nu,2}$, except that the challenge ciphertext is a semi-functional encryption of a random message in G_T and under two random identities in $\mathbb{Z}_q$. We denote the challenge ciphertext in $\mathsf{Game}_{\mathsf{Final}}$ as $\mathsf{CT}^{(\mathsf{R})}_{ek_{\sigma_\mathsf{R}},\mathsf{rcv}_\mathsf{R}}$.

We prove following lemmas to show the above games are indistinguishable by following an analogous strategy of [13,19,20]. 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 $\mathsf{Game}_{\mathsf{Real}}$ 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 gaps between $\mathsf{Game}_{\kappa\text{-}1,2}$ and $\mathsf{Game}_{\kappa,1}$, and between $\mathsf{Game}_{\kappa,1}$ and $\mathsf{Game}_{\kappa,2}$ are 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 $\mathsf{Game}_{\nu,2}$ to $\mathsf{Game}_{\mathsf{Final}}$ in one step, i.e., we show the joint distributions of

$$\left(\mathsf{mpk}, \mathsf{CT}^{(\mathsf{SF})}_{ek_{\sigma^*_\beta},\mathsf{rcv}^*_\beta}, \left\{\mathsf{dk}^{(\mathsf{SF})}_{\rho_\ell}\right\}_{\ell\in[\nu]}\right) \quad \text{and} \quad \left(\mathsf{mpk}, \mathsf{CT}^{(\mathsf{R})}_{ek_{\sigma_\mathsf{R}},\mathsf{rcv}_\mathsf{R}}, \left\{\mathsf{dk}^{(\mathsf{SF})}_{\rho_\ell}\right\}_{\ell\in[\nu]}\right)$$

are equivalent for the adversary's view.

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

Lemma 3. *Suppose that there exists an adversary $\mathcal{A}$ where $|\mathsf{Adv}^{\mathsf{Game}_{\mathsf{Real}}}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{\mathsf{Game}_0}_{\mathcal{A}}(\lambda)| = \epsilon$. Then there exists an algorithm $\mathcal{B}_0$ such that $\mathsf{Adv}^{\mathsf{DS1}}_{\mathcal{B}_0}(\lambda) = \epsilon - 2/q$, with $K = 4$ and $N = 8$.*

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

$$D := \left(\mathbb{G}; g_2^{\mathbf{b}_1^*}, g_2^{\mathbf{b}_2^*}, g_2^{\mathbf{b}_3^*}, g_2^{\mathbf{b}_4^*}, g_1^{\mathbf{b}_1}, \ldots, g_1^{\mathbf{b}_8}, U_1, U_2, U_3, U_4, \mu_2\right)$$

along with (T_1, T_2, T_3, T_4). And in D we have that $U_1 = g_2^{\mu_1 \mathbf{b_1^*} + \mu_2 \mathbf{b_5^*}}, U_2 = g_2^{\mu_1 \mathbf{b_2^*} + \mu_2 \mathbf{b_6^*}}, U_3 = g_2^{\mu_1 \mathbf{b_3^*} + \mu_2 \mathbf{b_7^*}}, U_4 = g_2^{\mu_1 \mathbf{b_4^*} + \mu_2 \mathbf{b_8^*}}$. We require that $\mathcal{B}_0$ decides whether (T_1, T_2, T_3, T_4) are distributed as

$$(g_1^{\tau_1 \mathbf{b}_1}, g_1^{\tau_1 \mathbf{b}_2}, g_1^{\tau_1 \mathbf{b}_3}, g_1^{\tau_1 \mathbf{b}_4}) \quad \text{or} \quad (g_1^{\tau_1 \mathbf{b}_1 + \tau_2 \mathbf{b}_5}, g_1^{\tau_1 \mathbf{b}_2 + \tau_2 \mathbf{b}_6}, g_1^{\tau_1 \mathbf{b}_3 + \tau_2 \mathbf{b}_7}, g_1^{\tau_1 \mathbf{b}_4 + \tau_2 \mathbf{b}_8}).$$

$\mathcal{B}_0$ simulates $\mathsf{Game}_{\mathsf{Real}}$ or Game_0 with $\mathcal{A}$ depending on the distribution of (T_1, T_2, T_3, T_4). To compute the master public key and master secret key, $\mathcal{B}_0$

chooses a random invertible matrix $\mathbf{A} \in \mathbb{Z}_q^{4\times 4}$. We then implicitly set dual orthonormal bases $\mathbb{D}, \mathbb{D}^*$ to:

$$\mathbf{d}_1 := \mathbf{b}_1, \dots, \mathbf{d}_4 := \mathbf{b}_4, \quad (\mathbf{d}_5, \dots, \mathbf{d}_8) := (\mathbf{b}_5, \dots, \mathbf{b}_8)\mathbf{A},$$
$$\mathbf{d}_1^* := \mathbf{b}_1^*, \dots, \mathbf{d}_4^* := \mathbf{b}_4^*, \quad (\mathbf{d}_5^*, \dots, \mathbf{d}_8^*) := (\mathbf{b}_5^*, \dots, \mathbf{b}_8^*)(\mathbf{A}^{-1})^\top.$$

We note that $\mathbb{D}, \mathbb{D}^*$ are properly distributed, and reveal no information about $\mathbf{A}$. Moreover, $\mathcal{B}_0$ cannot generate $g_2^{\mathbf{d}_5^*}, g_2^{\mathbf{d}_6^*}, g_2^{\mathbf{d}_7^*}, g_2^{\mathbf{d}_8^*}$, but these will not be needed for creating normal keys. $\mathcal{B}_0$ chooses random value $\alpha, \eta \in \mathbb{Z}_q$ and computes $g_T := e(g_1, g_2)^{\mathbf{d}_1 \cdot \mathbf{d}_1^*}$. It then gives $\mathcal{A}$ the master public key

$$\mathsf{mpk} := \left\{ \mathbb{G}; g_T^\alpha, g_T^\eta, g_1^{\mathbf{d_1}}, g_1^{\mathbf{d_2}} \right\}.$$

The master secret key

$$\mathsf{msk} := \left\{ \alpha, \eta, g_1^{\mathbf{d_3}}, g_1^{\mathbf{d_4}}, g_2^{\mathbf{d_1^*}}, g_2^{\mathbf{d_2^*}}, g_2^{\mathbf{d_3^*}}, g_2^{\mathbf{d_4^*}} \right\}$$

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 $(m_0, \mathsf{rcv}_0^*, \sigma_0^*)$ and $(m_1, \mathsf{rcv}_1^*, \sigma_1^*)$. $\mathcal{B}_0$ chooses a random bit $\beta \in \{0,1\}$ and picks $r' \xleftarrow{R} \mathbb{Z}_q$ and then encrypts m_β under rcv_β^* and $ek_{\sigma_\beta^*}$ as follows:

$$ek_{\sigma_\beta^*} := g_1^{\eta\mathbf{b_3}}(T_3^{\sigma_\beta^*} \cdot T_4^{-1})^{r'},$$
$$\mathsf{C} := m_\beta \cdot \left(e(T_1, g_2^{\mathbf{b_1^*}}) \right)^\alpha = m_\beta \cdot (g_T^\alpha)^z,$$
$$\mathsf{C}_0 := ek_{\sigma_\beta^*} \cdot T_1 \cdot T_2^{\mathsf{rcv}_\beta^*} = g_1^{\eta\mathbf{b_3}}(T_3^{\sigma_\beta^*} \cdot T_4^{-1})^{r'} \cdot T_1 \cdot T_2^{\mathsf{rcv}_\beta^*},$$

where $\mathcal{B}_0$ has implicitly set $r := r'\tau_1$ and $z := \tau_1$. It gives the ciphertext $ct = (\mathsf{C}, \mathsf{C}_0)$ to $\mathcal{A}$.

Now, if (T_1, T_2, T_3, T_4) are equal to $(g_1^{\tau_1\mathbf{b}_1}, g_1^{\tau_1\mathbf{b}_2}, g_1^{\tau_1\mathbf{b}_3}, g_1^{\tau_1\mathbf{b}_4})$, then this is a properly distributed normal encryption of m_β. In this case, $\mathcal{B}_0$ has properly simulated $\mathsf{Game}_{\mathsf{Real}}$. If (T_1, T_2, T_3, T_4) are equal to $(g_1^{\tau_1\mathbf{b}_1+\tau_2\mathbf{b}_5}, g_1^{\tau_1\mathbf{b}_2+\tau_2\mathbf{b}_6}, g_1^{\tau_1\mathbf{b}_3+\tau_2\mathbf{b}_7}, g_1^{\tau_1\mathbf{b}_4+\tau_2\mathbf{b}_8})$ instead, then the ciphertext element C_0 has an additional term of

$$\tau_2(\mathbf{b_5} + \mathsf{rcv}_\beta^*\mathbf{b_6}) + r'\tau_2(\sigma_\beta^*\mathbf{b_7} - \mathbf{b_8})$$

in its exponent. The coefficients here in the basis $\mathbf{b}_5, \mathbf{b}_6, \mathbf{b}_7, \mathbf{b}_8$ form the vector $\tau_2(1, \mathsf{rcv}_\beta^*, r'\sigma_\beta^*, -r')$. To compute the coefficients in the basis $\mathbf{d}_5, \mathbf{d}_6, \mathbf{d}_7, \mathbf{d}_8$, we multiply the matrix $\mathbf{A}^{-1}$ by the transpose of this vector, obtaining the new vector $\tau_2\mathbf{A}^{-1}(1, \mathsf{rcv}_\beta^*, r'\sigma_\beta^*, -r')^\top$. Since $\mathbf{A}$ is random (everything else given to $\mathcal{A}$ has been distributed independently of $\mathbf{A}$), these coefficients are uniformly random except with probability $2/q$ (namely, the cases τ_2 defined in Subspace problem is zero, (r_5, r_6, r_7, r_8) defined in Equation 3 is the zero vector) from Lemma 2. 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 $\mathsf{Game}_{\mathsf{Real}}$ and Game_0 to achieve an advantage $\epsilon - \frac{2}{q}$ against the subspace assumption in G_1, namely $\mathsf{Adv}_{\mathcal{B}_0}^{\mathsf{DS1}}(\lambda) = \epsilon - \frac{2}{q}$. □

Lemma 4. *Suppose that there exists an adversary $\mathcal{A}$ where $|\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_{\kappa\text{-}1,2}}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_{\kappa,1}}(\lambda)| = \epsilon$. Then there exists an algorithm $\mathcal{B}_{\kappa,1}$ such that $\mathsf{Adv}_{\mathcal{B}_{\kappa,1}}^{\mathsf{DS2}}(\lambda) = \epsilon - 6/q$, with $K = 4$ and $N = 8$.*

Proof. $\mathcal{B}_{\kappa,1}$ is given

$$D := \left(\mathbb{G}; g_1^{\mathbf{b}_1}, g_1^{\mathbf{b}_2}, g_1^{\mathbf{b}_3}, g_1^{\mathbf{b}_4}, g_2^{\mathbf{b}_1^*}, \ldots, g_2^{\mathbf{b}_8^*}, U_1, U_2, U_3, U_4, \mu_2\right)$$

along with (T_1, T_2, T_3, T_4). And in D we have that $U_1 = g_1^{\mu_1\mathbf{b_1}+\mu_2\mathbf{b_5}}, U_2 = g_1^{\mu_1\mathbf{b_2}+\mu_2\mathbf{b_6}}, U_3 = g_1^{\mu_1\mathbf{b_3}+\mu_2\mathbf{b_7}}, U_4 = g_1^{\mu_1\mathbf{b_4}+\mu_2\mathbf{b_8}}$. We require that $\mathcal{B}_{\kappa,1}$ decides whether (T_1, T_2, T_3, T_4) are distributed as

$$(g_2^{\tau_1\mathbf{b}_1^*}, g_2^{\tau_1\mathbf{b}_2^*}, g_2^{\tau_1\mathbf{b}_3^*}, g_2^{\tau_1\mathbf{b}_4^*}) \quad \text{or} \quad (g_2^{\tau_1\mathbf{b}_1^*+\tau_2\mathbf{b}_5^*}, g_2^{\tau_1\mathbf{b}_2^*+\tau_2\mathbf{b}_6^*}, g_2^{\tau_1\mathbf{b}_3^*+\tau_2\mathbf{b}_7^*}, g_2^{\tau_1\mathbf{b}_4^*+\tau_2\mathbf{b}_8^*}).$$

$\mathcal{B}_{\kappa,1}$ simulates $\mathsf{Game}_{\kappa\text{-}1,2}$ or $\mathsf{Game}_{\kappa,1}$ with $\mathcal{A}$ depending on the distribution of (T_1, T_2, T_3, T_4). To compute the master public key and master secret key, $\mathcal{B}_{\kappa,1}$ chooses a random invertible matrix $\mathbf{A} \in \mathbb{Z}_q^{4\times 4}$. We then implicitly set dual orthonormal bases $\mathbb{D}, \mathbb{D}^*$ to:

$$\begin{aligned} &\mathbf{d}_1 := \mathbf{b}_1, \ldots, \mathbf{d}_4 := \mathbf{b}_4, \quad (\mathbf{d}_5, \ldots, \mathbf{d}_8) := (\mathbf{b}_5, \ldots, \mathbf{b}_8)\mathbf{A}, \\ &\mathbf{d}_1^* := \mathbf{b}_1^*, \ldots, \mathbf{d}_4^* := \mathbf{b}_4^*, \quad (\mathbf{d}_5^*, \ldots, \mathbf{d}_8^*) := (\mathbf{b}_5^*, \ldots, \mathbf{b}_8^*)(\mathbf{A}^{-1})^\top. \end{aligned}$$

We note that $\mathbb{D}, \mathbb{D}^*$ are properly distributed, and reveal no information about $\mathbf{A}$. $\mathcal{B}_{\kappa,1}$ chooses random value $\alpha, \eta \in \mathbb{Z}_q$ and compute $g_T := e(g_1, g_2)^{\mathbf{d}_1\cdot\mathbf{d}_1^*}$. It then gives $\mathcal{A}$ the master public key

$$\mathsf{mpk} := \left\{\mathbb{G}; g_T^\alpha, g_T^\eta, g_1^{\mathbf{d_1}}, g_1^{\mathbf{d_2}}\right\}.$$

The master secret key

$$\mathsf{msk} := \left\{\alpha, \eta, g_1^{\mathbf{d_3}}, g_1^{\mathbf{d_4}}, g_2^{\mathbf{d_1^*}}, g_2^{\mathbf{d_2^*}}, g_2^{\mathbf{d_3^*}}, g_2^{\mathbf{d_4^*}}\right\}$$

is known to $\mathcal{B}_{\kappa,1}$, which allows $\mathcal{B}_{\kappa,1}$ to respond to all of $\mathcal{A}$'s key queries by calling the normal key generation algorithm. Since $\mathcal{B}_{\kappa,1}$ also knows $g_2^{\mathbf{d}_5^*}, g_2^{\mathbf{d}_6^*}, g_2^{\mathbf{d}_7^*}, g_2^{\mathbf{d}_8^*}$, it can easily produce (inter) semi-functional keys. To answer the first κ-1 key queries that $\mathcal{A}$ makes, $\mathcal{B}_{\kappa,1}$ runs the $\mathsf{KeyGenSF}$ algorithm to produce semi-functional keys and gives these to $\mathcal{A}$. To answer the κ-th key query for ρ_κ, $\mathcal{B}_{\kappa,1}$ picks $s, s_2 \xleftarrow{R} \mathbb{Z}_q$ and responds with:

$$\mathsf{dk}_{\rho_\kappa} := \left\{k_1 = g_2^{\alpha\mathbf{b_1^*}+s\mathbf{b_3^*}} \cdot (T_1^{\rho_\kappa} T_2^{-1}),\ k_2 = g_2^{s_2(\rho_\kappa\mathbf{b_1^*}-\mathbf{b_2^*})+s\mathbf{b_4^*}},\ k_3 = (g_T^\eta)^s\right\}.$$

Noting that k_2 is a normal key, $\mathcal{B}_{\kappa,1}$ needs to determine whether k_1 is semi-functional or normal key and this implicitly sets $s_1 := \tau_1$. If (T_1, T_2, T_3, T_4) are equal to $(g_2^{\tau_1\mathbf{b}_1^*}, g_2^{\tau_1\mathbf{b}_2^*}, g_2^{\tau_1\mathbf{b}_3^*}, g_2^{\tau_1\mathbf{b}_4^*})$, then this is a properly distributed normal key.

If (T_1, T_2, T_3, T_4) are equal to $(g_2^{\tau_1 \mathbf{b}_1^* + \tau_2 \mathbf{b}_5^*}, g_2^{\tau_1 \mathbf{b}_2^* + \tau_2 \mathbf{b}_6^*}, g_2^{\tau_1 \mathbf{b}_3^* + \tau_2 \mathbf{b}_7^*}, g_2^{\tau_1 \mathbf{b}_4^* + \tau_2 \mathbf{b}_8^*})$, then this is a inter-semi-functional key, whose exponent vector includes

$$\tau_2(\rho_\kappa \mathbf{b_5}^* - \mathbf{b_6}^* + 0 \cdot \mathbf{b_7}^* + 0 \cdot \mathbf{b_8}^*) \tag{4}$$

as its component in the span of $\mathbf{b}_5^*, \mathbf{b}_6^*, \mathbf{b}_7^*, \mathbf{b}_8^*$. To respond to the remaining key queries, $\mathcal{B}_{\kappa,1}$ simply runs the normal key generation algorithm.

At some point, $\mathcal{A}$ sends $\mathcal{B}_{\kappa,1}$ two pairs $(m_0, \mathsf{rcv}_0^*, \sigma_0^*)$ and $(m_1, \mathsf{rcv}_1^*, \sigma_1^*)$. $\mathcal{B}_{\kappa,1}$ chooses a random bit $\beta \in \{0,1\}$ and picks $r' \xleftarrow{R} \mathbb{Z}_q$ and then encrypts m_β under rcv_β^* and $ek_{\sigma_\beta^*}$ as follows:

$$ek_{\sigma_\beta^*} := g_1^{\eta \mathbf{b_3}} (U_3^{\sigma_\beta^*} \cdot U_4^{-1})^{r'},$$

$$\mathsf{C} := m_\beta \cdot \left(e(U_1, g_2^{\mathbf{b_1^*}})\right)^\alpha = m_\beta \cdot (g_T^\alpha)^z,$$

$$\mathsf{C}_0 := ek_{\sigma_\beta^*} \cdot U_1 \cdot U_2^{\mathsf{rcv}_\beta^*} = g_1^{\eta \mathbf{b_3}} (U_3^{\sigma_\beta^*} \cdot U_4^{-1})^{r'} \cdot U_1 \cdot U_2^{\mathsf{rcv}_\beta^*},$$

where $\mathcal{B}_{\kappa,1}$ has implicitly set $r := r'\mu_1$ and $z := \mu_1$. The "semi-functional part" of the exponent vector here is:

$$\mu_2(\mathbf{b_5} + \mathsf{rcv}_\beta^* \mathbf{b_6}) + r'\mu_2(\sigma_\beta^* \mathbf{b_7} - \mathbf{b_8}) \tag{5}$$

We observe that if $\mathsf{rcv}_\beta^* = \rho_\kappa$ (which is not allowed) and the decryption algorithm gives an attribute snd_κ that can correctly decrypt the ciphertext, i.e., $\mathsf{snd}_\kappa = \sigma_\beta^*$, then vectors in Equations 4 and 5 would be orthogonal in the decryption algorithm, resulting in a nominally semi-functional ciphertext and key pair. It gives the ciphertext $ct = (\mathsf{C}, \mathsf{C}_0)$ to $\mathcal{A}$.

We now argue that since $\mathsf{rcv}_\beta^* \neq \rho_\kappa$, in $\mathcal{A}$'s view the vectors in Equations 4 and 5 are distributed as random vectors in the spans of $\mathbf{d}_5^*, \mathbf{d}_6^*, \mathbf{d}_7^*, \mathbf{d}_8^*$ and $\mathbf{d}_5, \mathbf{d}_6, \mathbf{d}_7, \mathbf{d}_8$ respectively. To see this, we take the coefficients of vectors in Equations 4 and 5 in terms of the bases $\mathbf{b}_5^*, \mathbf{b}_6^*, \mathbf{b}_7^*, \mathbf{b}_8^*$ and $\mathbf{b}_5, \mathbf{b}_6, \mathbf{b}_7, \mathbf{b}_8$ respectively and translate them into coefficients in terms of the bases $\mathbf{d}_5^*, \mathbf{d}_6^*, \mathbf{d}_7^*, \mathbf{d}_8^*$ and $\mathbf{d}_5, \mathbf{d}_6, \mathbf{d}_7, \mathbf{d}_8$. Using the change of basis matrix $\mathbf{A}$, we obtain the new coefficients (in vector form) as:

$$\tau_2 \mathbf{A}^\top (\rho_\kappa, -1, 0, 0)^\top, \quad \mu_2 \mathbf{A}^{-1} (1, \mathsf{rcv}_\beta^*, r'\sigma_\beta^*, -r')^\top.$$

Since the distribution of everything given to $\mathcal{A}$ except for the κ-th key and the challenge ciphertext is independent of the random matrix $\mathbf{A}$ and $\mathsf{rcv}_\beta^* \neq \rho_\kappa$, we can conclude that these coefficients are uniformly except with probability $4/q$ (namely, the cases τ_2 or μ_2 defined in Subspace problem is zero, $\{s_{i,1}\}_{i=5,\ldots,8}$ or (r_5, r_6, r_7, r_8) defined in Equations 1 and 3 is the zero vector) from Lemma 2. Thus, $\mathcal{B}_{\kappa,1}$ has properly simulated $\mathsf{Game}_{\kappa,1}$ in this case.

If (T_1, T_2, T_3, T_4) are equal to $(g_2^{\tau_1 \mathbf{b}_1^*}, g_2^{\tau_1 \mathbf{b}_2^*}, g_2^{\tau_1 \mathbf{b}_3^*}, g_2^{\tau_1 \mathbf{b}_4^*})$, then the coefficients of the vector in Equation 5 are uniformly except with probability $2/q$ (namely, the cases μ_2 defined in Subspace problem is zero, (r_5, r_6, r_7, r_8) defined in Equation 3 is the zero vector) from Lemma 2. Thus, $\mathcal{B}_{\kappa,1}$ has properly simulated $\mathsf{Game}_{\kappa\text{-}1,2}$ in this case.

In summary, $\mathcal{B}_{\kappa,1}$ has properly simulated either $\mathsf{Game}_{\kappa\text{-}1,2}$ or $\mathsf{Game}_{\kappa,1}$ for $\mathcal{A}$, depending on the distribution of (T_1, T_2, T_3, T_4). It can therefore leverage $\mathcal{A}$'s advantage ϵ between these games to obtain an advantage $\epsilon - 6/q$ against the Subspace assumption in G_2, namely $\mathsf{Adv}^{\mathsf{DS2}}_{\mathcal{B}_{\kappa,1}}(\lambda) = \epsilon - 6/q$. □

Lemma 5. *Suppose that there exists an adversary $\mathcal{A}$ where $|\mathsf{Adv}^{\mathsf{Game}_{\kappa,1}}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{\mathsf{Game}_{\kappa,2}}_{\mathcal{A}}(\lambda)| = \epsilon$. Then there exists an algorithm $\mathcal{B}_{\kappa,2}$ such that $\mathsf{Adv}^{\mathsf{DS2}}_{\mathcal{B}_{\kappa,2}}(\lambda) = \epsilon - 6/q$, with $K = 4$ and $N = 8$.*

Proof. This proof is very similar to the proof of the previous lemma and $\mathcal{B}_{\kappa,2}$ is given

$$D := \left(\mathbb{G}; g_1^{\mathbf{b_1}}, g_1^{\mathbf{b_2}}, g_1^{\mathbf{b_3}}, g_1^{\mathbf{b_4}}, g_2^{\mathbf{b}_1^*}, \ldots, g_2^{\mathbf{b}_8^*}, U_1, U_2, U_3, U_4, \mu_2\right)$$

along with (T_1, T_2, T_3, T_4). And in D we have that $U_1 = g_1^{\mu_1 \mathbf{b_1} + \mu_2 \mathbf{b_5}}, U_2 = g_1^{\mu_1 \mathbf{b_2} + \mu_2 \mathbf{b_6}}, U_3 = g_1^{\mu_1 \mathbf{b_3} + \mu_2 \mathbf{b_7}}, U_4 = g_1^{\mu_1 \mathbf{b_4} + \mu_2 \mathbf{b_8}}$. We require that $\mathcal{B}_{\kappa,2}$ decides whether (T_1, T_2, T_3, T_4) are distributed as

$$(g_2^{\tau_1 \mathbf{b}_1^*}, g_2^{\tau_1 \mathbf{b}_2^*}, g_2^{\tau_1 \mathbf{b}_3^*}, g_2^{\tau_1 \mathbf{b}_4^*}) \quad \text{or} \quad (g_2^{\tau_1 \mathbf{b}_1^* + \tau_2 \mathbf{b}_5^*}, g_2^{\tau_1 \mathbf{b}_2^* + \tau_2 \mathbf{b}_6^*}, g_2^{\tau_1 \mathbf{b}_3^* + \tau_2 \mathbf{b}_7^*}, g_2^{\tau_1 \mathbf{b}_4^* + \tau_2 \mathbf{b}_8^*}).$$

$\mathcal{B}_{\kappa,2}$ simulates $\mathsf{Game}_{\kappa,1}$ or $\mathsf{Game}_{\kappa,2}$ with $\mathcal{A}$ depending on the distribution of (T_1, T_2, T_3, T_4). To compute the master public key and master secret key, $\mathcal{B}_{\kappa,2}$ chooses a random invertible matrix $\mathbf{A} \in \mathbb{Z}_q^{4\times 4}$. We then implicitly set dual orthonormal bases $\mathbb{D}, \mathbb{D}^*$ to:

$$\begin{aligned} &\mathbf{d}_1 := \mathbf{b}_1, \ldots, \mathbf{d}_4 := \mathbf{b}_4, \quad (\mathbf{d}_5, \ldots, \mathbf{d}_8) := (\mathbf{b}_5, \ldots, \mathbf{b}_8)\mathbf{A}, \\ &\mathbf{d}_1^* := \mathbf{b}_1^*, \ldots, \mathbf{d}_4^* := \mathbf{b}_4^*, \quad (\mathbf{d}_5^*, \ldots, \mathbf{d}_8^*) := (\mathbf{b}_5^*, \ldots, \mathbf{b}_8^*)(\mathbf{A}^{-1})^{\top}. \end{aligned}$$

We note that $\mathbb{D}, \mathbb{D}^*$ are properly distributed, and reveal no information about $\mathbf{A}$. $\mathcal{B}_{\kappa,2}$ chooses random value $\alpha, \eta \in \mathbb{Z}_q$ and compute $g_T := e(g_1, g_2)^{\mathbf{d}_1 \cdot \mathbf{d}_1^*}$. It then gives $\mathcal{A}$ the master public key

$$\mathsf{mpk} := \left\{\mathbb{G}; g_T^{\alpha}, g_T^{\eta}, g_1^{\mathbf{d_1}}, g_1^{\mathbf{d_2}}\right\}.$$

The master secret key

$$\mathsf{msk} := \left\{\alpha, \eta, g_1^{\mathbf{d_3}}, g_1^{\mathbf{d_4}}, g_2^{\mathbf{d_1^*}}, g_2^{\mathbf{d_2^*}}, g_2^{\mathbf{d_3^*}}, g_2^{\mathbf{d_4^*}}\right\}$$

is known to $\mathcal{B}_{\kappa,2}$, which allows $\mathcal{B}_{\kappa,2}$ to respond to all of $\mathcal{A}$'s key queries by calling the normal key generation algorithm. Since $\mathcal{B}_{\kappa,2}$ also knows $g_2^{\mathbf{d}_5^*}, g_2^{\mathbf{d}_6^*}, g_2^{\mathbf{d}_7^*}, g_2^{\mathbf{d}_8^*}$, it can easily produce (inter) semi-functional keys. To answer the first κ-1 key queries that $\mathcal{A}$ makes, $\mathcal{B}_{\kappa,2}$ runs the $\mathsf{KeyGenSF}$ algorithm to produce semi-functional keys and gives these to $\mathcal{A}$. To answer the κ-th key query for ρ_κ,

$\mathcal{B}_{\kappa,2}$ picks $s, s_1, \{s_{i,1}\}_{i=5,\ldots,8} \xleftarrow{R} \mathbb{Z}_q$ and responds with:

$$\mathsf{dk}_{\rho_\kappa} := \{k_1 = g_2^{\alpha \mathbf{d}_1^* + s_1(\rho \mathbf{d}_1^* - \mathbf{d}_2^*) + s\mathbf{d}_\mathbf{3}^* + [s_{5,1}\mathbf{d}_5^* + s_{6,1}\mathbf{d}_6^* + s_{7,1}\mathbf{d}_\mathbf{7}^*]},$$
$$k_2 = g_2^{s\mathbf{b}_\mathbf{4}^*} \cdot (T_1^{\rho_\kappa} T_2^{-1}), \quad k_3 = (g_T^\eta)^s\}.$$

Noting that k_1 is a semi-functional key, $\mathcal{B}_{\kappa,2}$ needs to determine whether k_2 is semi-functional or normal key and this implicitly sets $s_2 := \tau_1$. If (T_1, T_2, T_3, T_4) are equal to $(g_2^{\tau_1 \mathbf{b}_1^*}, g_2^{\tau_1 \mathbf{b}_2^*}, g_2^{\tau_1 \mathbf{b}_3^*}, g_2^{\tau_1 \mathbf{b}_4^*})$, then this is a properly distributed normal key. If (T_1, T_2, T_3, T_4) are equal to $(g_2^{\tau_1 \mathbf{b}_1^* + \tau_2 \mathbf{b}_5^*}, g_2^{\tau_1 \mathbf{b}_2^* + \tau_2 \mathbf{b}_6^*}, g_2^{\tau_1 \mathbf{b}_3^* + \tau_2 \mathbf{b}_7^*}, g_2^{\tau_1 \mathbf{b}_4^* + \tau_2 \mathbf{b}_8^*})$, then this is a semi-functional key, whose exponent vector includes

$$\tau_2(\rho_\kappa \mathbf{b_5}^* - \mathbf{b_6}^* + 0 \cdot \mathbf{b_7}^* + 0 \cdot \mathbf{b_8}^*) \tag{6}$$

as its component in the span of $\mathbf{b}_5^*, \mathbf{b}_6^*, \mathbf{b}_7^*, \mathbf{b}_8^*$. To respond to the remaining key queries, $\mathcal{B}_{\kappa,2}$ simply runs the normal key generation algorithm.

At some point, $\mathcal{A}$ sends $\mathcal{B}_{\kappa,2}$ two pairs $(m_0, \mathsf{rcv}_0^*, \sigma_0^*)$ and $(m_1, \mathsf{rcv}_1^*, \sigma_1^*)$. $\mathcal{B}_{\kappa,2}$ chooses a random bit $\beta \in \{0,1\}$ and picks $r' \xleftarrow{R} \mathbb{Z}_q$ and then encrypts m_β under rcv_β^* and $ek_{\sigma_\beta^*}$ as follows:

$$ek_{\sigma_\beta^*} := g_1^{\eta \mathbf{b_3}} (U_3^{\sigma_\beta^*} \cdot U_4^{-1})^{r'},$$

$$\mathsf{C} := m_\beta \cdot \left(e(U_1, g_2^{\mathbf{b}_\mathbf{1}^*})\right)^\alpha = m_\beta \cdot (g_T^\alpha)^z,$$

$$\mathsf{C}_0 := ek_{\sigma_\beta^*} \cdot U_1 \cdot U_2^{\mathsf{rcv}_\beta^*} = g_1^{\eta \mathbf{b_3}} (U_3^{\sigma_\beta^*} \cdot U_4^{-1})^{r'} \cdot U_1 \cdot U_2^{\mathsf{rcv}_\beta^*},$$

where $\mathcal{B}_{\kappa,2}$ has implicitly set $r := r'\mu_1$ and $z := \mu_1$. The "semi-functional part" of the exponent vector here is:

$$\mu_2(\mathbf{b_5} + \mathsf{rcv}_\beta^* \mathbf{b_6}) + r'\mu_2(\sigma_\beta^* \mathbf{b_7} - \mathbf{b_8}) \tag{7}$$

We observe that if $\mathsf{rcv}_\beta^* = \rho_\kappa$ (which is not allowed) and the decryption algorithm gives an attribute snd_κ that can correctly decrypt the ciphertext, i.e., $\mathsf{snd}_\kappa = \sigma_\beta^*$, then vectors in Equations 6 and 7 would be orthogonal in the decryption algorithm, resulting in a nominally semi-functional ciphertext and key pair. It gives the ciphertext $ct = (\mathsf{C}, \mathsf{C}_0)$ to $\mathcal{A}$.

We now argue that since $\mathsf{rcv}_\beta^* \neq \rho_\kappa$, in $\mathcal{A}$'s view the vectors in Equations 6 and 7 are distributed as random vectors in the spans of $\mathbf{d}_5^*, \mathbf{d}_6^*, \mathbf{d}_7^*, \mathbf{d}_8^*$ and $\mathbf{d}_5, \mathbf{d}_6, \mathbf{d}_7, \mathbf{d}_8$ respectively. To see this, we take the coefficients of vectors in Equations 6 and 7 in terms of the bases $\mathbf{b}_5^*, \mathbf{b}_6^*, \mathbf{b}_7^*, \mathbf{b}_8^*$ and $\mathbf{b}_5, \mathbf{b}_6, \mathbf{b}_7, \mathbf{b}_8$ respectively and translate them into coefficients in terms of the bases $\mathbf{d}_5^*, \mathbf{d}_6^*, \mathbf{d}_7^*, \mathbf{d}_8^*$ and $\mathbf{d}_5, \mathbf{d}_6, \mathbf{d}_7, \mathbf{d}_8$. Using the change of basis matrix $\mathbf{A}$, we obtain the new coefficients (in vector form) as:

$$\tau_2 \mathbf{A}^\top (\rho_\kappa, -1, 0, 0)^\top, \quad \mu_2 \mathbf{A}^{-1} (1, \mathsf{rcv}_\beta^*, r'\sigma_\beta^*, -r')^\top.$$

Since the distribution of everything given to $\mathcal{A}$ except for the κ-th key and the challenge ciphertext is independent of the random matrix $\mathbf{A}$ and $\mathsf{rcv}_\beta^* \neq \rho_\kappa$, we can conclude that these coefficients are uniformly except with probability $4/q$ (namely, the cases τ_2 or μ_2 defined in Subspace problem is zero, $\{s_{i,j}\}_{i=5,\ldots,8;j=1,2}$ or (r_5, r_6, r_7, r_8) defined in Equations 2 and 3 is the zero vector) from Lemma 2. Thus, $\mathcal{B}_{\kappa,2}$ has properly simulated $\mathsf{Game}_{\kappa,2}$ in this case.

If (T_1, T_2, T_3, T_4) are equal to $(g_2^{\tau_1 \mathbf{b}_1^*}, g_2^{\tau_1 \mathbf{b}_2^*}, g_2^{\tau_1 \mathbf{b}_3^*}, g_2^{\tau_1 \mathbf{b}_4^*})$, then the coefficients of the vector in Equation 7 are uniformly except with probability $2/q$ (namely, the cases μ_2 defined in Subspace problem is zero, (r_5, r_6, r_7, r_8) defined in Equation 3 is the zero vector) from Lemma 2. Thus, $\mathcal{B}_{\kappa,2}$ has properly simulated $\mathsf{Game}_{\kappa,1}$ in this case.

In summary, $\mathcal{B}_{\kappa,2}$ has properly simulated either $\mathsf{Game}_{\kappa,1}$ or $\mathsf{Game}_{\kappa,2}$ for $\mathcal{A}$, depending on the distribution of (T_1, T_2, T_3, T_4). It can therefore leverage $\mathcal{A}$'s advantage ϵ between these games to obtain an advantage $\epsilon - 6/q$ against the Subspace assumption in G_2, namely $\mathsf{Adv}_{\mathcal{B}_{\kappa,2}}^{\mathsf{DS2}}(\lambda) = \epsilon - 6/q$. □

Lemma 6. *For any adversary $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Final}}}(\lambda) \leq \mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_{\nu,2}}(\lambda) + 1/q$.*

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

$$\left(\mathsf{mpk}, \mathsf{CT}^{(\mathsf{SF})}_{ek_{\sigma_\beta^*}, \mathsf{rcv}_\beta^*}, \left\{\mathsf{dk}^{(\mathsf{SF})}_{\rho_\ell}\right\}_{\ell\in[\nu]}\right)$$

in $\mathsf{Game}_{\nu,2}$ and that of

$$\left(\mathsf{mpk}, \mathsf{CT}^{(\mathsf{R})}_{ek_{\sigma_\mathsf{R}}, \mathsf{rcv}_\mathsf{R}}, \left\{\mathsf{dk}^{(\mathsf{SF})}_{\rho_\ell}\right\}_{\ell\in[\nu]}\right)$$

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

For this purpose, we pick $\mathbf{A} := (\xi_{i,j}) \xleftarrow{R} \mathbb{Z}_q^{4\times 4}$ and define new dual orthonormal bases $\mathbb{F} := (\mathbf{f}_1, \ldots, \mathbf{f}_8)$, and $\mathbb{F}^* := (\mathbf{f}_1^*, \ldots, \mathbf{f}_8^*)$ as follows:

$$\begin{pmatrix} \mathbf{f}_1 \\ \mathbf{f}_2 \\ \mathbf{f}_3 \\ \mathbf{f}_4 \\ \mathbf{f}_5 \\ \mathbf{f}_6 \\ \mathbf{f}_7 \\ \mathbf{f}_8 \end{pmatrix} := \begin{pmatrix} 1 & 0 & 0 & 0 & 0\,0\,0\,0 \\ 0 & 1 & 0 & 0 & 0\,0\,0\,0 \\ 0 & 0 & 1 & 0 & 0\,0\,0\,0 \\ 0 & 0 & 0 & 1 & 0\,0\,0\,0 \\ \xi_{1,1} & \xi_{1,2} & \xi_{1,3} & \xi_{1,4} & 1\,0\,0\,0 \\ \xi_{2,1} & \xi_{2,2} & \xi_{2,3} & \xi_{2,4} & 0\,1\,0\,0 \\ \xi_{3,1} & \xi_{3,2} & \xi_{3,3} & \xi_{3,4} & 0\,0\,1\,0 \\ \xi_{4,1} & \xi_{4,2} & \xi_{4,3} & \xi_{4,4} & 0\,0\,0\,1 \end{pmatrix} \begin{pmatrix} \mathbf{d}_1 \\ \mathbf{d}_2 \\ \mathbf{d}_3 \\ \mathbf{d}_4 \\ \mathbf{d}_5 \\ \mathbf{d}_6 \\ \mathbf{d}_7 \\ \mathbf{d}_8 \end{pmatrix},$$

$$\begin{pmatrix} \mathbf{f}_1^* \\ \mathbf{f}_2^* \\ \mathbf{f}_3^* \\ \mathbf{f}_4^* \\ \mathbf{f}_5^* \\ \mathbf{f}_6^* \\ \mathbf{f}_7^* \\ \mathbf{f}_8^* \end{pmatrix} := \begin{pmatrix} 1\,0\,0\,0 & -\xi_{1,1} & -\xi_{2,1} & -\xi_{3,1} & -\xi_{4,1} \\ 0\,1\,0\,0 & -\xi_{1,2} & -\xi_{2,2} & -\xi_{3,2} & -\xi_{4,2} \\ 0\,0\,1\,0 & -\xi_{1,3} & -\xi_{2,3} & -\xi_{3,3} & -\xi_{4,3} \\ 0\,0\,0\,1 & -\xi_{1,4} & -\xi_{2,4} & -\xi_{3,4} & -\xi_{4,4} \\ 0\,0\,0\,0 & 1 & 0 & 0 & 0 \\ 0\,0\,0\,0 & 0 & 1 & 0 & 0 \\ 0\,0\,0\,0 & 0 & 0 & 1 & 0 \\ 0\,0\,0\,0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \mathbf{d}_1^* \\ \mathbf{d}_2^* \\ \mathbf{d}_3^* \\ \mathbf{d}_4^* \\ \mathbf{d}_5^* \\ \mathbf{d}_6^* \\ \mathbf{d}_7^* \\ \mathbf{d}_8^* \end{pmatrix}.$$

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 master public key, challenge ciphertext, and queried secret keys, $(\mathsf{mpk}, \mathsf{CT}^{(\mathsf{SF})}_{ek_{\sigma^*_\beta}, \mathsf{rcv}^*_\beta}, \{\mathsf{dk}^{(\mathsf{SF})}_{\rho_\ell}\}_{\ell\in[\nu]})$ in $\mathsf{Game}_{\nu,2}$ are expressed over bases $\mathbb{D}$ and $\mathbb{D}^*$ as

$$\begin{aligned} \mathsf{mpk} &:= \left\{\mathbb{G}; g_T^\alpha, g_T^\eta, g_1^{\mathbf{d_1}}, g_1^{\mathbf{d_2}}\right\}, \quad ek_{\sigma^*_\beta} := g_1^{\eta\mathbf{d_3}+r(\sigma^*_\beta\mathbf{d_3}-\mathbf{d_4})}, \\ \mathsf{CT}^{(\mathsf{SF})}_{ek_{\sigma^*_\beta}, \mathsf{rcv}^*_\beta} &:= \{\mathsf{C} = m\cdot(g_T^\alpha)^z, \\ &\qquad \mathsf{C}_0 = ek_{\sigma^*_\beta}\cdot g_1^{z(\mathbf{d_1}+\mathsf{rcv}^*_\beta\mathbf{d_2})+[r_5\mathbf{d_5}+r_6\mathbf{d_6}+r_7\mathbf{d_7}+r_8\mathbf{d_8}]} \\ &\qquad\quad = g_1^{\eta\mathbf{d_3}+r(\sigma^*_\beta\mathbf{d_3}-\mathbf{d_4})+z(\mathbf{d_1}+\mathsf{rcv}^*_\beta\mathbf{d_2})+[r_5\mathbf{d_5}+r_6\mathbf{d_6}+r_7\mathbf{d_7}+r_8\mathbf{d_8}]}\}, \end{aligned}$$

$$\begin{aligned} \mathsf{dk}^{(\mathsf{SF})}_{\rho_\ell} := \{k_1 &= g_2^{\alpha\mathbf{d_1}^*+s_{1,\ell}(\rho_\ell\mathbf{d_1}^*-\mathbf{d_2}^*)+s_\ell\mathbf{d_3}^*+[s_{5,1,\ell}\mathbf{d_5}^*+s_{6,1,\ell}\mathbf{d_6}^*+s_{7,1,\ell}\mathbf{d_7}^*]}, \\ k_2 &= g_2^{s_{2,\ell}(\rho_\ell\mathbf{d_1}^*-\mathbf{d_2}^*)+s_\ell\mathbf{d_4}^*+[s_{5,2,\ell}\mathbf{d_5}^*+s_{6,2,\ell}\mathbf{d_6}^*+s_{8,2,\ell}\mathbf{d_8}^*]}, \\ k_3 &= (g_T^\eta)^s\ \}_{\ell\in[\nu]}. \end{aligned}$$

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

$$\begin{aligned} \mathsf{mpk} &:= \left\{\mathbb{G}; g_T^\alpha, g_T^\eta, g_1^{\mathbf{f_1}}, g_1^{\mathbf{f_2}}\right\}, \quad ek_{\sigma^*_\beta} := g_1^{\eta\mathbf{d_3}+r(\sigma^*_\beta\mathbf{d_3}-\mathbf{d_4})}, \\ \mathsf{CT}^{(\mathsf{R})}_{ek_{\sigma_\mathsf{R}}, \mathsf{rcv}_\mathsf{R}} &:= \{\mathsf{C} = m\cdot(g_T^\alpha)^z, \\ &\qquad \mathsf{C}_0 = ek_{\sigma^*_\beta}\cdot g_1^{z(\mathbf{d_1}+\mathsf{rcv}^*_\beta\mathbf{d_2})+[r_5\mathbf{d_5}+r_6\mathbf{d_6}+r_7\mathbf{d_7}+r_8\mathbf{d_8}]} \\ &\qquad\quad = g_1^{\eta\mathbf{f_3}+(r_3\mathbf{f_3}+r_4\mathbf{f_4}+r_1\mathbf{f_1}+r_2\mathbf{f_2})+[r_5\mathbf{f_5}+r_6\mathbf{f_6}+r_7\mathbf{f_7}+r_8\mathbf{f_8}]}\}, \end{aligned}$$

$$\begin{aligned} \mathsf{dk}^{(\mathsf{SF})}_{\rho_\ell} := \{k_1 &= g_2^{\alpha\mathbf{f_1}^*+s_{1,\ell}(\rho_\ell\mathbf{f_1}^*-\mathbf{f_2}^*)+s_\ell\mathbf{f_3}^*+[t_{5,1,\ell}\mathbf{f_5}^*+t_{6,1,\ell}\mathbf{f_6}^*+t_{7,1,\ell}\mathbf{f_7}^*+t_{8,1,\ell}\mathbf{f_8}^*]}, \\ k_2 &= g_2^{s_{2,\ell}(\rho_\ell\mathbf{f_1}^*-\mathbf{f_2}^*)+s_\ell\mathbf{f_4}^*+[t_{5,2,\ell}\mathbf{f_5}^*+t_{6,2,\ell}\mathbf{f_6}^*+t_{7,2,\ell}\mathbf{f_7}^*+t_{8,2,\ell}\mathbf{f_8}^*]}, \\ k_3 &= (g_T^\eta)^s\ \}_{\ell\in[\nu]}. \end{aligned}$$

where

$$\begin{aligned}
r_1 &:= z - r_5\xi_{1,1} - r_6\xi_{2,1} - r_7\xi_{3,1} - r_8\xi_{4,1},\\
r_2 &:= z \cdot \mathsf{rcv}^*_\beta - r_5\xi_{1,2} - r_6\xi_{2,2} - r_7\xi_{3,2} - r_8\xi_{4,2},\\
r_3 &:= r \cdot \sigma^*_\beta - r_5\xi_{1,3} - r_6\xi_{2,3} - r_7\xi_{3,3} - r_8\xi_{4,3},\\
r_4 &:= -r - r_5\xi_{1,4} - r_6\xi_{2,4} - r_7\xi_{3,4} - r_8\xi_{4,4};
\end{aligned}$$

$$\left\{\begin{aligned}
t_{5,1,\ell} &:= \alpha \cdot \xi_{1,1} + s_{1,\ell}\rho_\ell \cdot \xi_{1,1} - s_{1,\ell} \cdot \xi_{1,2} + s_\ell \cdot \xi_{1,3} + s_{5,1,\ell}\\
t_{6,1,\ell} &:= \alpha \cdot \xi_{2,1} + s_{1,\ell}\rho_\ell \cdot \xi_{2,1} - s_{1,\ell} \cdot \xi_{2,2} + s_\ell \cdot \xi_{2,3} + s_{6,1,\ell}\\
t_{7,1,\ell} &:= \alpha \cdot \xi_{3,1} + s_{1,\ell}\rho_\ell \cdot \xi_{3,1} - s_{1,\ell} \cdot \xi_{3,2} + s_\ell \cdot \xi_{3,3} + s_{7,1,\ell}\\
t_{8,1,\ell} &:= \alpha \cdot \xi_{4,1} + s_{1,\ell}\rho_\ell \cdot \xi_{4,1} - s_{1,\ell} \cdot \xi_{4,2} + s_\ell \cdot \xi_{4,3}
\end{aligned}\right\}_{\ell\in[\nu]},$$

$$\left\{\begin{aligned}
t_{5,2,\ell} &:= s_{2,\ell}\rho_\ell \cdot \xi_{1,1} - s_{2,\ell} \cdot \xi_{1,2} + s_\ell \cdot \xi_{1,4} + s_{5,2,\ell}\\
t_{6,2,\ell} &:= s_{2,\ell}\rho_\ell \cdot \xi_{2,1} - s_{2,\ell} \cdot \xi_{2,2} + s_\ell \cdot \xi_{2,4} + s_{6,2,\ell}\\
t_{7,2,\ell} &:= s_{2,\ell}\rho_\ell \cdot \xi_{3,1} - s_{2,\ell} \cdot \xi_{3,2} + s_\ell \cdot \xi_{3,4}\\
t_{8,2,\ell} &:= s_{2,\ell}\rho_\ell \cdot \xi_{4,1} - s_{2,\ell} \cdot \xi_{4,2} + s_\ell \cdot \xi_{4,4} + s_{8,2,\ell}
\end{aligned}\right\}_{\ell\in[\nu]},$$

which are all uniformly distributed if (r_5, r_6, r_7, r_8) defined in Equation 3 is a non-zero vector, since $\big(z, r, \{\xi_{i,j}\}_{i\in[4],j\in[4]}, \{s_{i,j,\ell}\}_{i=5,\ldots,8;j=1,2;\ell\in[\nu]}\big)$ are all uniformly picked from $\mathbb{Z}_q$.

In other words, the coefficients $(z, z\cdot\mathsf{rcv}^*_\beta, r\sigma^*_\beta, -r)$ of $\mathbf{d}_1, \mathbf{d}_2, \mathbf{d}_3, \mathbf{d}_4$ in the C_0 term of the challenge ciphertext is changed to random coefficients $(r_1, r_2, r_3, r_4) \in \mathbb{Z}_q^4$ of $\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3, \mathbf{f}_4$, thus the challenge ciphertext can be viewed as a semi-functional encryption of a random message in G_T and under two random identities in $\mathbb{Z}_q$. Moreover, all coefficients $\{t_{i,j,\ell}\}_{i=5,\ldots,8;j=1,2;\ell\in[\nu]}$ of $\mathbf{f}^*_5, \mathbf{f}^*_6, \mathbf{f}^*_7, \mathbf{f}^*_8$ in the $\{\mathsf{dk}^{(\mathsf{SF})}_{\rho_\ell}\}_{\ell\in[\nu]}$ are all uniformly distributed since $\{s_{i,j,\ell}\}_{i=5,\ldots,8;j=1,2;\ell\in[\nu]}$ of $\mathbf{d}^*_5, \mathbf{d}^*_6, \mathbf{d}^*_7, \mathbf{d}^*_8$ are all independent random values. Thus

$$\left(\mathsf{mpk}, \mathsf{CT}^{(\mathsf{SF})}_{ek_{\sigma^*_\beta}, \mathsf{rcv}^*_\beta}, \left\{\mathsf{dk}^{(\mathsf{SF})}_{\rho_\ell}\right\}_{\ell\in[\nu]}\right)$$

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

$$\left(\mathsf{mpk}, \mathsf{CT}^{(\mathsf{R})}_{ek_{\sigma_\mathsf{R}}, \mathsf{rcv}_\mathsf{R}}, \left\{\mathsf{dk}^{(\mathsf{SF})}_{\rho_\ell}\right\}_{\ell\in[\nu]}\right)$$

in $\mathsf{Game}_{\mathsf{Final}}$.

In the adversary's view, both $(\mathbb{D}, \mathbb{D}^*)$ and $(\mathbb{F}, \mathbb{F}^*)$ are consistent with the same master public key. Therefore, the challenge ciphertext and queried secret keys above can be expressed as keys and ciphertext in two ways, in $\mathsf{Game}_{\nu,2}$ over bases $(\mathbb{D}, \mathbb{D}^*)$ and in $\mathsf{Game}_{\mathsf{Final}}$ over bases $(\mathbb{F}, \mathbb{F}^*)$. Thus, $\mathsf{Game}_{\nu,2}$ and $\mathsf{Game}_{\mathsf{Final}}$ are statistically indistinguishable except with probability $1/q$ (namely, the case (r_5, r_6, r_7, r_8) defined in Equation 3 is the zero vector). □

Lemma 7. *For any adversary $\mathcal{A}$, $\mathsf{Adv}^{\mathsf{Game}_{\mathsf{Final}}}_{\mathcal{A}}(\lambda) = 0$.*

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

In $\mathsf{Game}_{\mathsf{Final}}$, the challenge ciphertext is a semi-functional encryption of a random message in G_T and under two random identities in $\mathbb{Z}_q$, independent of the two messages and the challenge identities provided by $\mathcal{A}$. Thus, our IB-ME scheme satisfies the privacy property defined in Def. 8 under the SXDH assumption.

Theorem 2. *The proposed IB-ME scheme satisfies authenticity under the Symmetric External Diffie-Hellman assumption. More precisely, for any PPT adversary $\mathcal{A}$ break the authenticity of our IB-ME scheme, its advantage* $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{ib\text{-}auth}}}(\lambda)$ *is negligible.*

Proof. The authenticity property intuitively says that if an adversary does not hold the corresponding encryption key ek_σ produced by the challenger, it cannot compute a valid ciphertext under the identity σ. Thus, it is corresponding to the unforgeability of signature, and we can directly reduce the authenticity to the security of the IBE system.

Assume that there is a PPT adversary $\mathcal{A}$ which breaks the authenticity property with advantage ϵ, we then employ it to build another PPT algorithm $\mathcal{B}$ to break a fully secure IBE system which consists of the following algorithms:

- $\mathsf{IBE.Setup}(1^\lambda)$: The same as the Setup algorithm, except that the master public key is $mpk := \{\mathbb{G}; \alpha, g_T^\alpha, g_T^\eta, g_1^{\mathbf{d_1}}, g_1^{\mathbf{d_2}}, g_2^{\mathbf{d_1^*}}, g_2^{\mathbf{d_2^*}}, g_2^{\mathbf{d_3^*}}, g_2^{\mathbf{d_4^*}}\}$, and the master secret key is $msk := \{\eta, g_1^{\mathbf{d_3}}, g_1^{\mathbf{d_4}}\}$.
- $\mathsf{IBE.KeyGen}(msk, \sigma)$: The same as the SKGen algorithm, and the secret key is $sk_\sigma := g_1^{\eta\mathbf{d_3}+r(\sigma\mathbf{d_3}-\mathbf{d_4})}$.
- $\mathsf{IBE.Enc}(mpk, \sigma, m)$: Similar to the RKGen algorithm, and the ciphertext is $ct := \{\mathsf{C} = m \cdot (g_T^\eta)^s, \mathsf{C}_0 = g_2^{s(\mathbf{d_3^*}+\sigma\mathbf{d_4^*})}\}$.
- $\mathsf{IBE.Dec}(mpk, sk_\sigma, ct)$: Compute the message as $m := \mathsf{C}/e(\mathsf{C}_0, sk_\sigma)$.

Oracles $\mathsf{O}_1, \mathsf{O}_2$ are implemented by $\mathsf{SKGen}(\mathsf{mpk}, \mathsf{msk}, \cdot)$ and $\mathsf{RKGen}(\mathsf{mpk}, \mathsf{msk}, \cdot)$ and are simulated by $\mathcal{B}$ as follows:

1. $\mathsf{SKGen}(\mathsf{mpk}, \mathsf{msk}, \cdot)$: $\mathcal{A}$ launches a query for identity σ to O_1,then $\mathcal{B}$ transfers this identity σ to the IBE system for generating secret key. It uses the $\mathsf{IBE.KeyGen}$ algorithm's output to answer this query and returns the secret key sk_σ to $\mathcal{B}$. Finally, $\mathcal{B}$ uses this secret key sk_σ from IBE as ek_σ to answer $\mathcal{A}$'s query for the encryption key.
2. $\mathsf{RKGen}(\mathsf{mpk}, \mathsf{msk}, \cdot)$: $\mathcal{A}$ launches a query for identity ρ to O_2,then $\mathcal{B}$ transfers this identity ρ to the IBE system. It uses mpk (in IBE) to generate the corresponding keys, randomly picks $s, s_1, s_2 \overset{R}{\leftarrow} \mathbb{Z}_q$, computes

$$k_1 = g_2^{\alpha\mathbf{d_1^*}+s_1(\rho\mathbf{d_1^*}-\mathbf{d_2^*})+s\mathbf{d_3^*}}, k_2 = g_2^{s_2(\rho\mathbf{d_1^*}-\mathbf{d_2^*})+s\mathbf{d_4^*}}, k_3 = (g_T^\eta)^s,$$

and returns these keys to $\mathcal{B}$. Finally, $\mathcal{B}$ uses $dk_\rho = \{k_1, k_2, k_3\}$ to answer $\mathcal{A}$'s query for the decryption key.

Suoopse that $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{ib-auth}}}(\lambda) = \epsilon$, where ϵ is a non-negligible value. Then we can build an algorithm $\mathcal{B}$ whose $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{IBE}}(\lambda) = \epsilon$ as follow:

Upon $\mathcal{A}$ making a query of (σ, ρ), $\mathcal{B}$ generates the encryption key and decryption key to answer this query by simulating $\mathsf{O}_1, \mathsf{O}_2$, and sends (ek_σ, dk_ρ) back to $\mathcal{A}$. Then $\mathcal{A}$ can find another $\sigma^* \neq \mathsf{snd}$ with ϵ probability such that σ^* is also valid for decryption of ct, and sends σ^* to $\mathcal{B}$. Note that the fact snd and σ^* are both valid for $ct_{\sigma,\mathsf{rcv}}$ implies for a ciphertext associated with σ in the underlying IBE, there would be two different secret keys associated with snd and σ^* respectively. The sk_{σ^*} in IBE is identical to the ek_{σ^*} in IB-ME. Therefore, $\mathcal{B}$ can make secret key query for snd, and challenge (m_0, σ_0) and (m_1, σ^*). Then $\mathcal{B}$ can distinguish the challenge ciphertext easily by using the secret key associated with σ^* and break this IBE system.

This means that by this simulation, we have successfully reduced the authenticity of IB-ME to the security of this IBE system. And we have

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{ib-auth}}}(\lambda) \leq \mathsf{Adv}_{\mathcal{B}}^{\mathsf{IBE}}(\lambda).$$

That is to say, if an adversary cannot successfully break the IBE system we constructed, it cannot forge a valid ciphertext in our IB-ME scheme either. We show that this IBE system is fully secure in the full version [11], i.e., the advantage of $\mathcal{B}$ winning the IBE game defined in Def. 5 is negligible. Thus for any PPT adversary $\mathcal{A}$, its advantage of breaking the authenticity property of our IB-ME scheme is negligible. □

Note that we have challenged m and σ at the same time, but in fact, we do not need to challenge identity σ at all. That is to say the security of a trivial IBE is sufficient and anonymity is not required. Because another $\sigma^* \neq \mathsf{snd}$ can be obtained from $\mathcal{A}$ during the proof, and $\mathcal{B}$ sends identity snd and (m_0, m_1) to the challenger, the same result can be obtained.

5 Conclusion

In this paper, we propose the first identity-based matchmaking encryption scheme under the standard assumptions in the standard model. We construct our IB-ME scheme by a variant of two-level anonymous IBE, which is based on Okamoto and Takashima's dual pairing vector spaces, and its security reductions rely on Waters's dual system encryption under the SXDH assumption. Our directly constructed scheme does not rely on other cryptographic tools such as non-interactive zero-knowledge proof systems. Meanwhile, we leave several questions. First, although all parameters in our scheme have constant numbers of group elements, the size should be shorter and the number of pairing for decryption should be reduced to improve efficiency. Second, construct IB-ME schemes that satisfy the enhanced privacy [16] under standard assumptions. Third, practical extensions such as revocability and traceability are further works.

Acknowledgements We are extremely grateful to the editors and anonymous reviewers for their insightful and constructive comments on this work. Jie Chen is supported by National Natural Science Foundation of China (61972156), NSFC-ISF Joint Scientific Research Program (61961146004), National Key Research and Development Program of China (2018YFA0704701) and Innovation Program of Shanghai Municipal Education Commission (2021-01-07-00-08-E00101). Jinming Wen is partially supported by National Natural Science Foundation of China (No.11871248), Guangdong Major Project of Basic and Applied Basic Research (2019B030302008), and Natural Science Foundation of Guangdong Province of China (2021A515010857, 2022A1515010029). Jian Weng is supported by Major Program of Guangdong Basic and Applied Research Project under Grant No.2019B030302008, National Natural Science Foundation of China under Grant No.61825203, Guangdong Provincial Science and Technology Project under Grant No.2021A0505030033, National Joint Engineering Research Center of Network Security Detection and Protection Technology, and Guangdong Key Laboratory of Data Security and Privacy Preserving.

References

1. Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Kohno, T., Lange, T., Malone-Lee, J., Neven, G., Paillier, P., Shi, H.: Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions. J. Cryptol. **21**(3), 350–391 (2008), https://doi.org/10.1007/s00145-007-9006-6
2. Agrawal, S., Boneh, D., Boyen, X.: Efficient lattice (H)IBE in the standard model. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 553–572. Springer, Berlin, Heidelberg (2010), https://doi.org/10.1007/978-3-642-13190-5_28
3. Ateniese, G., Francati, D., Nuñez, D., Venturi, D.: Match me if you can: Matchmaking encryption and its applications. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019, Part II. LNCS, vol. 11693, pp. 701–731. Springer, Cham (2019), https://doi.org/10.1007/978-3-030-26951-7_24
4. Attrapadung, N.: Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 557–577. Springer, Berlin, Heidelberg (2014), https://doi.org/10.1007/978-3-642-55220-5_31
5. Boneh, D., Boyen, X.: Efficient selective-id secure identity-based encryption without random oracles. In: Cachin, C., Camenisch, J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Berlin, Heidelberg (2004), https://doi.org/10.1007/978-3-540-24676-3_14
6. Boneh, D., Boyen, X.: Secure identity based encryption without random oracles. In: Franklin, M.K. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 443–459. Springer, Berlin, Heidelberg (2004), https://doi.org/10.1007/978-3-540-28628-8_27
7. Boneh, D., Franklin, M.K.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Berlin, Heidelberg (2001), https://doi.org/10.1007/3-540-44647-8_13
8. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the weil pairing. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 514–532. Springer, Berlin, Heidelberg (2001), https://doi.org/10.1007/3-540-45682-1_30
9. Cash, D., Hofheinz, D., Kiltz, E., Peikert, C.: Bonsai trees, or how to delegate a lattice basis. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110,

pp. 523–552. Springer, Berlin, Heidelberg (2010), https://doi.org/10.1007/978-3-642-13190-5_27

10. Chen, J., Gay, R., Wee, H.: Improved dual system ABE in prime-order groups via predicate encodings. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part II. LNCS, vol. 9057, pp. 595–624. Springer, Berlin, Heidelberg (2015), https://doi.org/10.1007/978-3-662-46803-6_20
11. Chen, J., Li, Y., Wen, J., Weng, J.: Identity-based matchmaking encryption from standard assumptions. IACR Cryptology ePrint Archive (2022)
12. Chen, J., Lim, H.W., Ling, S., Wang, H., Wee, H.: Shorter IBE and signatures via asymmetric pairings. In: Abdalla, M., Lange, T. (eds.) Pairing-Based Cryptography - Pairing 2012. LNCS, vol. 7708, pp. 122–140. Springer, Berlin, Heidelberg (2012), https://doi.org/10.1007/978-3-642-36334-4_8
13. Chen, J., Lim, H.W., Ling, S., Wang, H., Wee, H.: Shorter identity-based encryption via asymmetric pairings. Des. Codes Cryptogr. **73**(3), 911–947 (2014), https://doi.org/10.1007/s10623-013-9834-3
14. Chen, J., Wee, H.: Fully, (almost) tightly secure IBE and dual system groups. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II. LNCS, vol. 8043, pp. 435–460. Springer, Berlin, Heidelberg (2013), https://doi.org/10.1007/978-3-642-40084-1_25
15. Cocks, C.C.: An identity based encryption scheme based on quadratic residues. In: Honary, B. (ed.) Cryptography and Coding, 8th IMA International Conference, Cirencester, UK, December 17-19, 2001, Proceedings. LNCS, vol. 2260, pp. 360–363. Springer (2001), https://doi.org/10.1007/3-540-45325-3_32
16. Francati, D., Guidi, A., Russo, L., Venturi, D.: Identity-based matchmaking encryption without random oracles. In: Adhikari, A., Küsters, R., Preneel, B. (eds.) INDOCRYPT 2021. LNCS, vol. 13143, pp. 415–435. Springer, Cham (2021), https://doi.org/10.1007/978-3-030-92518-5_19
17. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Dwork, C. (ed.) Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008. pp. 197–206. STOC '08, ACM (2008), https://doi.org/10.1145/1374376.1374407
18. Goldwasser, S., Micali, S., Rivest, R.L.: A digital signature scheme secure against adaptive chosen-message attacks. SIAM J. Comput. **17**(2), 281–308 (1988), https://doi.org/10.1137/0217017
19. Lewko, A.B.: Tools for simulating features of composite order bilinear groups in the prime order setting. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 318–335. Springer, Berlin, Heidelberg (2012), https://doi.org/10.1007/978-3-642-29011-4_20
20. Lewko, A.B., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 62–91. Springer, Berlin, Heidelberg (2010), https://doi.org/10.1007/978-3-642-13190-5_4
21. Lewko, A.B., Waters, B.: New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 455–479. Springer, Berlin, Heidelberg (2010), https://doi.org/10.1007/978-3-642-11799-2_27
22. Lewko, A.B., Waters, B.: Decentralizing attribute-based encryption. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 568–588. Springer, Berlin, Heidelberg (2011), https://doi.org/10.1007/978-3-642-20465-4_31

23. Lewko, A.B., Waters, B.: Unbounded HIBE and attribute-based encryption. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 547–567. Springer, Berlin, Heidelberg (2011), https://doi.org/10.1007/978-3-642-20465-4_30
24. Lewko, A.B., Waters, B.: New proof methods for attribute-based encryption: Achieving full security through selective techniques. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 180–198. Springer, Berlin, Heidelberg (2012), https://doi.org/10.1007/978-3-642-32009-5_12
25. Okamoto, T., Takashima, K.: Homomorphic encryption and signatures from vector decomposition. In: Galbraith, S.D., Paterson, K.G. (eds.) Pairing-Based Cryptography - Pairing 2008. LNCS, vol. 5209, pp. 57–74. Springer, Berlin, Heidelberg (2008), https://doi.org/10.1007/978-3-540-85538-5_4
26. Okamoto, T., Takashima, K.: Hierarchical predicate encryption for inner-products. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 214–231. Springer, Berlin, Heidelberg (2009), https://doi.org/10.1007/978-3-642-10366-7_13
27. Okamoto, T., Takashima, K.: Fully secure functional encryption with general relations from the decisional linear assumption. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 191–208. Springer, Berlin, Heidelberg (2010), https://doi.org/10.1007/978-3-642-14623-7_11
28. Okamoto, T., Takashima, K.: Some key techniques on pairing vector spaces. In: Nitaj, A., Pointcheval, D. (eds.) AFRICACRYPT 2011. LNCS, vol. 6737, pp. 380–382. Springer, Berlin, Heidelberg (2011), https://doi.org/10.1007/978-3-642-21969-6_25
29. Okamoto, T., Takashima, K.: Adaptively attribute-hiding (hierarchical) inner product encryption. In: Pointcheval, D., Johansson, T. (eds.) AEUROCRYPT 2012. LNCS, vol. 7237, pp. 591–608. Springer, Berlin, Heidelberg (2012), https://doi.org/10.1007/978-3-642-29011-4_35
30. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Berlin, Heidelberg (1984), https://doi.org/10.1007/3-540-39568-7_5
31. Waters, B.: Efficient identity-based encryption without random oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Berlin, Heidelberg (2005), https://doi.org/10.1007/11426639_7
32. Waters, B.: Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 619–636. Springer, Berlin, Heidelberg (2009), https://doi.org/10.1007/978-3-642-03356-8_36
33. Wee, H.: Dual system encryption via predicate encodings. In: Lindell, Y. (ed.) TCC 2014. LNCS, vol. 8349, pp. 616–637. Springer, Berlin, Heidelberg (2014), https://doi.org/10.1007/978-3-642-54242-8_26
34. Xu, S., Ning, J., Li, Y., Zhang, Y., Xu, G., Huang, X., Deng, R.H.: Match in my way: Fine-grained bilateral access control for secure cloud-fog computing. IEEE Trans. Dependable Secur. Comput. **19**(2), 1064–1077 (2022), https://doi.org/10.1109/TDSC.2020.3001557
35. Xu, S., Ning, J., Ma, J., Huang, X., Pang, H., Deng, R.H.: Expressive bilateral access control for internet-of-things in cloud-fog computing. In: Lobo, J., Pietro, R.D., Chowdhury, O., Hu, H. (eds.) SACMAT '21, Spain, June 16-18, 2021. pp. 143–154. ACM (2021), https://doi.org/10.1145/3450569.3463561