Oblivious Identity-based Encryption
(IBE Secure Against an Adversarial KGC)

Aikaterini Mitrokotsa[1], Sayantan Mukherjee[2], and Jenit Tomy[1]

[1] University of St. Gallen, St. Gallen, Switzerland
first.last@unisg.ch
[2] Indian Institute of Technology, Jammu, India
csayantan.mukherjee@gmail.com

Abstract. Identity-Based Encryption (IBE) was introduced in order to reduce the cost associated with Public Key Infrastructure systems. IBE allows users to request a trusted Key Generation Centre (KGC) for a secret key on a given identity, without the need to manage public keys. However, one of the main concerns of IBE is that the KGC has the power to decrypt all ciphertexts as it has access to all (identity, secret key) pairs. To address this issue, Chow (PKC 2009) introduced a new security property against the KGC by employing a new trusted party called Identity Certifying Authority (ICA). Emura *et al.* (ESORICS 2019) formalized this notion and proposed a construction in the random oracle model.
In this work, we first identify several existing IBE schemes where the KGC can decrypt a ciphertext even without knowing the receiver's identity. This paves the way for formalizing new capabilities for the KGC. We then propose a new security definition to capture an adversarial KGC including the newly identified capabilities and we remove the requirement of an additional trusted party. Finally, we propose a new IBE construction that allows users to ask the KGC for a secret key on an identity without leaking any information about the user's identity to the KGC. Our construction is provably secure in the standard model against an adversarial KGC and corrupted users. Furthermore, our construction is achieved in the composite order pairing groups and requires essentially optimal parameters.

Keywords: Identity-based Encryption · key escrow problem · pairing-based cryptography

1 Introduction

Public key cryptography has been widely employed in real-world applications. However, its use is accompanied by the need to process and store public key certificates under the public key infrastructure (PKI). Identity-based encryption (IBE) [21] has been introduced to reduce the cost associated with PKI systems, since it allows users to use arbitrary strings (*e.g.,* email addresses) as public keys. However, IBE requires a special entity called *key generation centre* (KGC), which maintains a master public and master secret key pair (mpk, msk), confirms the identity id of each user and generates a corresponding secret key sk_{id} using its master secret key. After retrieving the master public key from the KGC, anyone is able to encrypt messages for any user as long as the corresponding identity of the user is known.

However, this convenience of handling public keys in IBE comes at the cost of what is known as the *key escrow problem*, which is one of the main constraints in achieving widespread adoption of identity-based encryption (IBE). More precisely, since the Key Generation Centre (KGC) generates keys for a given identity, it has the power to decrypt all ciphertexts.

1.1 Current Solutions and Motivation

Several approaches were proposed to guarantee security against the adversarial KGC and to solve the key escrow problem. For instance, in *certificate-less encryption* [1], a user generates their own public/secret key pair (pk, sk) in addition to the KGC generated sk_{id}. While the encryption requires both the pk and the id, the decryption requires the sk_{id} (generated by the KGC) and the corresponding sk of the user. This restricts the KGC from decrypting ciphertexts, as it does not have access to the user's secret key sk. However, requiring a public key (pk) for encryption leads to public information that grows linearly with the number of users, contradicting the main advantage of IBE. Garg *et al.* [10,11] improved this shortcoming by introducing the notion of *registration-based encryption* (RBE) which allows the KGC to aggregate and compress the users' public keys to a master public key mpk. Instead of the KGC generating a secret key for each new user, the RBE KGC maintains the master public key mpk, and updates the mpk using the public key and the identity of the new user (pk, id). Thus, the encryption only requires the mpk and the id, while the decryption requires only sk. Goyal and Vusirikala [15] recently extended RBE by introducing verifiability in the key accumulation process in generating the mpk. The main disadvantage of RBE is that it requires periodic update of the mpk and the users need to receive this updated mpk in order to encrypt any message.

Another line of research attempted to address the key escrow problem by providing a level of anonymity to the ciphertexts. Intuitively, ciphertexts are kept anonymous, *i.e.* the KGC should not be able to determine the underlying identity used for the generation of a ciphertext. To capture this, Izabachène and Pointcheval [18] formalized the notion of *identity-based key encapsulation mechanisms* (IB-KEMs). However as pointed out by Chow [6], their definition is incomplete as they only allow the adversary to obtain the challenge ciphertext and not also the corresponding session key as in standard IB-KEM. Chow [6] attempted to address this issue by introducing a notion of security against the KGC, namely, *KGC anonymous ciphertext indistinguishability.* This security guarantee restricts the KGC from obtaining information about a plaintext from the corresponding ciphertext assuming that the user's identity is drawn uniformly at random and remains unknown to the KGC. However, according to the model proposed in [6] the KGC can keep a list of all the users' identities and corresponding secret keys (id, sk_{id}) and thus, could decrypt any ciphertext by performing a brute force attack on the ciphertext using the issued secret keys. In order to address this issue, Chow introduced a new entity called the identity-certifying authority (ICA) and an anonymous key-issuing protocol, which restricts the power of the KGC to recover information about the plaintexts but at the cost of placing a significant amount of trust on the ICA. In their analysis though, Chow defined the security of the IBE and that of an anonymous key-issuing protocol separately, with a rather informal treatment of the ICA when authenticating the users.

Emura *et al.* [8,9] tried to address this issue by defining an IBE scheme that resolves the key escrow problem and providing formal definitions of security against corrupted users, KGC and ICA and proposed two instantiations based on lattices and pairings. Their approach can be seen as a blind IBE with certified identities since they combine a blind IBE with an ICA in order to certify user identities, while the proposed constructions combine a standard anonymous IBE scheme with a blind signature scheme. Emura *et al.*'s work has been significant in formalizing a standard IBE scheme that captures the key escrow problem, while also proposing the first post-quantum IBE secure against a KGC; however, they still place a lot of trust in the ICA and their proposed constructions are secure in the random oracle model. Furthermore, in Emura *et al.*' constructions, a colluding ICA and KGC can also compute all the identity/secret-key pairs of all the identities. Another drawback of having two entities is that both entities, ICA and KGC need to be online during the key generation phase. In addition, the group-based construction of [8] is based on the Boneh-Franklin IBE [3] scheme, where the master secret key is x and the user secret key of identity id is $H(id)^x$. Although the constructions can be easily modified to have a construction without ICA, the security is still proven in the random-oracle model.
Another approach was the notion of blind identity-based encryption (blind IBE) introduced by Green and Hohenberger [17], which enables a key generator (*i.e.,* the KGC) to generate a secret key for a user identity, without revealing any information about the user's identity to the KGC. Camenisch *et al.* [4] introduced the notion of committed blind anonymous IBE, where anonymous refers to the fact that the ciphertext does not leak the identity that was used for its generation. Even though blind IBE schemes ensure that the identity of the user is hidden during the secret key generation, this guarantee is not sufficient for the KGC to not be able to decrypt the messages from the ciphertext. As a matter of fact, in these blind IBE schemes, the KGC can decrypt the messages from the ciphertexts using the master secret key without any knowledge of the underlying identity. We elaborate on the vulnerabilities of both of these schemes in Section 3.

Furthermore, Goyal introduced the notion of *Traceable Identity-based Encryption* [16] *i.e.,* one more IBE variant that considers the security against the KGC. However, this definition does not consider the security of ciphertexts against an adversarial KGC. We provide a comparison of the existing solutions in Figure 1.

Scheme	No ICA	Cipher-text Anonymity	Secret-key hidden from KGC/KC	Cipher-text security against KGC/KC	Security Model	Underlying Assumptions	Public parameters never modified
Chow[6]*	✗	✓	-	-	Standard	DBDH+	✓
Green *et.al.*[17]	✓	✗	✓	✗	Standard	DBDH+	✓
Camenish*et.al.*[4]	✓	✓	✓	✗	Standard	DBDH+	✓
Garg *et.al.*[10]	✓	✗	✓	✓	Standard	$i\mathcal{O}$	✗
Emura *et.al.* [8]	✗	✓	✓	✓	ROM	DBDH/LWE	✓
Garg *et.al.*[12]	✓	✓	✓	✓	Standard	CDH/LWE	✗
Glaeser *et.al.* [13]	✓	✓	✓	✓	Standard	DBDH+	✗
Ours	✓	✓	✓	✓	Standard	Subgroup Decision	✓

Fig. 1. Comparison with the existing solutions. ROM, DBDH, $i\mathcal{O}$, CDH, LWE stands for Random Oracle Model, Decision Bilinear Diffie-Hellman, Indistinguishability obfuscation, Computational Diffie-Hellman, and Learning with Errors respectively. *informal treatment of ICA in the security definition.

In this work, we revisit the problem of formally defining an IBE scheme that captures the key escrow problem and remains secure against an adversarial KGC, considering the standard model. More precisely, we address the following question:

Is it possible to provide an IBE construction that achieves security against an adversarial KGC without relying on an ICA or the random oracle assumption?

We answer this question affirmatively and we address the key escrow problem by introducing an anonymous IBE construction that provides strong security guarantees against an adversarial KGC in the standard model. To achieve that, we allow the user and the KGC to collaboratively generate a secret key corresponding to a user *id* (while blinding the user's *id*). More precisely, we combine the techniques from the Oblivious PRF (OPRF) protocol proposed by Jarecki and Liu [19], and Wee's IBE [23] in order to achieve an efficient and provably secure anonymous IBE in the standard model.

1.2 Our Contributions

Our contributions can be summarised as follows:
– We revisit some existing IBE schemes and identify a vulnerability that make them insecure against an adversarial KGC. More precisely, we identify several

existing IBE schemes, where the KGC can decrypt the ciphertext without even knowing the receiver's identity.
– We address the *key escrow problem* and provide a stronger definition against an adversarial KGC without requiring an additional entity *i.e.,* an identity-certifying authority (ICA) as required in previous work [6,8,9].
– We propose an anonymous IBE construction that provides strong security in the standard model against an adversarial KGC and corrupted users.
– Our IBE construction achieves high-efficiency guarantees since it relies on Wee's IBE construction [23]. More precisely, it requires essentially optimal parameters: the secret key is one group element, the overhead of ciphertext is one group element plus the size of π (where π denotes a PoK) and the decryption requires only one pairing.

1.3 Technical Overview

In a typical IBE scheme, the KGC is usually the most trusted entity that gets the identity of the users in plain and issues the corresponding keys. In this paper, we define and propose an IBE construction which is secure against an adversarial KGC along with the failed paths. We first observed that existing Blind IBE schemes [17,4] are insecure in the presence of an adversarial KGC even when the KGC does not know the challenge identity. We further observed this vulnerability in a few other standard IBE constructions [22,20] and therefore are not preferred as a candidate for an Oblivious IBE construction. Looking ahead, this vulnerability is mainly due to the fact that a linear reconstruction of the msk is performed during the decryption. That being said, we should mention that this is not a sufficient condition for our attack to hold. In Section 3.1, we describe this vulnerability with a few standard examples including the Blind IBEs [17,4] and some IBEs in the standard model [22,2,20]. To avoid this issue, we focus on an IBE that has a non-linear reconstruction of the msk. This is where we utilize the structural similarity between Dodis-Yampolskiy VRF [7] and Wee's IBE [23].

Another solution for the key-escrow problem was proposed by Emura *et al.* [8,9] where they introduced a trusted certification authority and provided two constructions in the new proposed model. Their bilinear-map-based construction is based on Boneh-Franklin IBE[3] where the master secret key is x and the secret key of identity id is $\mathsf{H}(id)^x$. This IBE can be easily converted to a blind IBE by modifying the message sent by the user to the KGC as $\mathsf{H}(id)^y$ where y is a random value chosen by the user. The user can recover their secret key after receiving $\mathsf{H}(id)^{xy}$ from the KGC and the scheme can be proven in the random oracle model. Our goal is to provide a construction that does not rely on an ICA or the random oracle model.

Before we informally describe our construction, we revisit the IBE construction proposed by Wee [23]. Firstly, Wee's IBE defines a KEM-ciphertext $ct = (g^{(\alpha+id)s}, e(g,u)^s)$ and a secret key $sk_{id} = u^{\frac{1}{\alpha+id}}$ for any identity id where $msk = (u, \alpha) \leftarrow G \times \mathbb{Z}_N$ and $s \leftarrow \mathbb{Z}_N$. We should note that our attack does not work against Wee's IBE. However, a problem remains *i.e.,* how to compute the sk_{id}, since the KGC must know the user's id in plain. To address this issue we incorporate an oPRF that allows the generation of the sk_{id} obliviously, *i.e.,* without the KGC finding out the key. Recall that Jarecki-Liu's [19] extended Dodis-Yampolskiy VRF [7] towards an oblivious evaluation of PRF. Thus, we borrow the idea from Jarecki-Liu's [19] to generate the sk_{id} as an output of oblivious PRF ($F(msk; id) = g^{\frac{1}{msk+id}}$). The secret key generation procedure in our IBE scheme is performed as follows:

- Assume the KGC runs an additive homomorphic encryption $\mathsf{HE} = (\mathsf{HE.Setup}, \mathsf{HE.KeyGen}, \mathsf{HE.Enc}, \mathsf{HE.Dec})$. Generates $(pk, sk) \leftarrow \mathsf{HE.KeyGen}$
- The KGC publishes $(pk_1, pk_2) = (pk, \mathsf{HE.Enc}(pk, \alpha))$ as part of the master public key (mpk) of the IBE scheme and keeps msk to itself.
- A user with identity id computes $R = \mathsf{HE.Enc}(pk_1, r \cdot id) \cdot {pk_2}^r = \mathsf{HE.Enc}(pk, r \cdot id + r \cdot \alpha)$ for $r \leftarrow \mathbb{Z}_N$.
- The KGC then decrypts R to retrieve $t = r(\alpha + id)$ and outputs $U = u^{1/t}$.
- Finally, the user computes $U^r = u^{\frac{1}{\alpha+id}} = sk_{id}$.

Here observe that the KGC does not get any information about id due to the fact that a uniformly at random r is used. Intuitively our KGC security argument, although it deals with a lot of details, essentially is based on the fact that KGC is oblivious to the user identity in the key generation process. Note that, in reality, an adversarial KGC is involved in multiple key generation protocols. To capture this, we first introduce our security model and then give formal security proof in the introduced model. Looking ahead, the KGC security argument allows the adversary (modeling the adversarial KGC) to get the msk. So, we base our argument on the knowledge of id on which sk_{id} is computed. For this, we repurpose Wee's [23] Déjà Q based dual system encryption technique. In particular, we show that all the secret keys generated by the KGC can be replaced by a random function applied on a different id. For user security, on the other hand, we modify [23]'s proof to include some extra elements (part of mpk) that are required in our constructions.

1.4 Organization of the paper

In Section 2, we define some standard notations and recall the definition of bilinear groups, our complexity assumptions and the employed homomorphic encryption. In Section 3, we first describe an attack that applies on several existing schemes and then give a new definition of IBE secured at the presence of an adversarial KGC. Next, in Section 4 we propose a novel IBE construction and give a rigorous proof of the construction in the standard model. Finally, in Section 5 we conclude the paper.

2 Preliminaries

Notations Here we denote $[a, b] = \{i \in \mathbb{N} : a \leq i \leq b\}$ and for any $n \in \mathbb{N}$, $[n] = [1, n]$. The security parameter is denoted by λ where $\lambda \in \mathbb{N}$. By $s \leftarrow S$, we denote a uniformly at random choice s from S. By $A \approx B$, we mean that no computational adversary can distinguish between the distributions A and B. We use $Adv_{\mathcal{A}}^{M,\Pi}$ to denote the advantage adversary $\mathcal{A}$ has against protocol Π in the security model M and Adv_a is used to denote the advantage of $\mathcal{A}$ to break the game a. Also, $\det(A)$ represents the determinant of the matrix A. The notation $\log(x)$ represents the logarithm of x with base 2.

2.1 Mathematical Tools and Assumptions

Let G, H and G_T be three commutative multiplicative groups of order $N = p_1p_2$ where p_1 and p_2 are large prime numbers. A map $e : G \times H \to G_T$ is called an admissible bilinear pairing if,

- (Bilinear) For all $g \in G$ and all $h \in H$, $e(g^a, h^b) = e(g, h)^{ab}$ for any $a, b \in \mathbb{N}$.
- (Non-degenerate) $e(g, h) = 1$ only if $g = 1$ or $h = 1$.
- (Computable) For all $g \in G$ and all $h \in H$, there is an efficient algorithm that computes $e(g, h)$.

We call G and H *source groups* and G_T is called the *target group*. In this work, we consider type-3 pairing, where we do not know an efficient isomorphism between G and H. We can write $G = G_{p_1}G_{p_2}$ and $H = H_{p_1}H_{p_2}$ where G_{p_1}, G_{p_2} (resp. H_{p_1}, H_{p_2}) are subgroups of G (resp. H) of order p_1, p_2 respectively. We consider $BG(p_1, p_2)$ as a composite order type-3 bilinear group generator. $BG(p_1, p_2)$ takes as input two primes (p_1, p_2) of length $\Theta(\lambda)$ and outputs $(e, g_1, h_1, N, G, H, G_T)$ where G, H and G_T are cyclic groups of order $N = p_1p_2$ and $e : G \times H \to G_T$ is a non-degenerate bilinear map.

Subgroup Decision Assumptions

- SD_1 for group G: The SD_1 problem in group G is defined as following.

  Given $g_1 \leftarrow G_{p_1}, h_1 \leftarrow H_{p_1}$, $Z \leftarrow G$; decide if $Z \in G_{p_1}$ or $Z \in G$.

  The advantage of a probabilistic polynomial time algorithm $\mathcal{A}$ to solve SD_1 in G is

  $$Adv_{\mathcal{A}}^{SD_1,G} = |Pr[\mathcal{A}(g_1, h_1, Z) = 1 : Z \in G_{p_1}] - Pr[\mathcal{A}(g_1, h_1, Z) = 1 : Z \in G]|$$

  where the probability is calculated over the random choice of $g_1 \in G_{p_1}$, $h_1 \in H_{p_1}$, $Z \in G$ as well as the random bits used by $\mathcal{A}$. The SD_1 assumption in G holds if for any probabilistic polynomial time algorithm $\mathcal{A}$, $Adv_{\mathcal{A}}^{SD_1,G} \leq$ negl(λ).
- SD_2 for group H: The SD_2 problem in group H is defined as following.

  Given $g_{\{1,2\}} \leftarrow G, h_1 \leftarrow H_{p_1}$, $Z \leftarrow H$; decide if $Z \in H_{p_1}$ or $Z \in H$.

  The advantage of a probabilistic polynomial time algorithm $\mathcal{A}$ to solve SD_2 in H is

  $$\begin{aligned} Adv_{\mathcal{A}}^{SD_2,H} =& |Pr[\mathcal{A}(g_{\{1,2\}}, h_1, Z) = 1 : Z \in H_{p_1}] \\ & - Pr[\mathcal{A}(g_{\{1,2\}}, h_1, Z) = 1 : Z \in H]| \end{aligned}$$

where the probability is calculated over the random choice of $g_{\{1,2\}} \in G$, $h_1 \in H_{p_1}$, $Z \in H$ as well as the random bits used by $\mathcal{A}$. The SD_2 assumption in H holds if for any probabilistic polynomial time algorithm $\mathcal{A}$, $Adv_{\mathcal{A}}^{SD_2,H} \leq$ negl(λ).

2.2 Additively Homomorphic Encryption with Additional Properties

This work requires an additively homomorphic encryption scheme with verifiable encryption. We borrow the definition from Jarecki and Liu [19]. For ease of use in our construction, we split the setup phase of Jarecki and Liu into two functions $\mathsf{Primes}, \mathsf{Setup}$ here.

- $\mathsf{Primes}(1^\lambda)$. It takes as input the security parameter 1^λ and outputs two primes p_1, p_2 of length $\Theta(\lambda)$.
- $\mathsf{Setup}(p_1, p_2)$. Generates the public parameter par from the inputs p_1, p_2.
- $\mathsf{KeyGen}(par)$. This function takes the public parameter par as input and outputs a random public/secret key pair (pk, sk).
- $\mathsf{Enc}(pk, m)$. Uses the public key pk and a message $m \in \mathcal{M}$ to compute a ciphertext C.
- $\mathsf{Dec}(sk, C)$. It takes the secret key sk and a ciphertext C to retrieve the underlying message m.

Besides semantic security, we require the following properties of the above encryption scheme:

- **Additive Homomorphism**: We require that there is an efficient publicly evaluable operation on ciphertexts, which for convenience, we denote as a multiplication, s.t. $\mathsf{Enc}(pk, m_0) \cdot \mathsf{Enc}(pk, m_1) \in \mathsf{Enc}(pk, m_0 + m_1)$. We can also define exponentiation and division operations on ciphertexts, and by homomorphism of the encryption $(\mathsf{Enc}(pk, m))^a = \mathsf{Enc}(pk, a \cdot m)$ and $\mathsf{Enc}(pk, m_0)/\mathsf{Enc}(pk, m_1) \in \mathsf{Enc}(pk, m_0 - m_1)$, for any a and any m, m_0, m_1 in $\mathcal{M}$.
- **Verifiable Encryption**: We require an efficient realization of the following proof system, given public keys pk and pk' and ciphertexts C_1, C_2 and C', where C_1 and C_2 are supposed to be ciphertexts under the public key pk.

$$\mathsf{PoK}\{m \mid \exists m' \in \mathbb{Z}_n, \text{ s.t. } C' = \mathsf{Enc}(pk', m') \wedge C_2 \in (C_1 \cdot \mathsf{Enc}(pk, m))^{m'}\}. \quad (1)$$

We instantiate the encryption scheme with additively homomorphic encryption of [19]. The details are provided in Appendix A.

3 Oblivious Identity-Based Encryption

In this section, we first describe the existing IBE schemes' weaknesses, then introduce a new IBE definition called Oblivious Identity-Based Encryption (OIBE). We aim to define a new IBE scheme that does not suffer from the identified weaknesses.

3.1 Vulnerability of Existing IBE schemes

We identified that multiple existing IBE constructions are vulnerable to an attack that an adversarial KGC can perform. One of the main approaches to achieve security against KGC is blind IBE. We analyze the existing blind IBE constructions in terms of KGC security. The description of the following schemes are similar to the notations mentioned in the preliminaries.

Green and Hohenberger [17]. The first Blind IBE construction was given by Green *et al.* which has public parameters $params$, master secret key msk, and the ciphertext of m for the identity id, defined as follows:

$$params = (g, g_1 = g^{\alpha}, g_2, h, F), msk = g_2^{\alpha}, ct_{id} = (m \cdot e(g_1, g_2)^t, g^t, F(id)^t)$$

The KGC can compute $e(g_1, g_2)^t = e(g^{\alpha}, g_2)^t = e(g^t, g_2^{\alpha})$ using the ciphertext and msk, and remove the mask $e(g_1, g_2)^t$ in the ciphertext to compute the message m. Here, the KGC can decrypt a ciphertext without knowing the underlying identity or the corresponding secret key.

Camenisch, Kohlweiss, Rial and Sheedy [4]. Another blind IBE construction by Camenisch *et al.* has $params, msk, sk_{id}$ as defined below:

$$params = (\Omega = e(g,h)^{t_1 t_2 \alpha}, g, h, g_0 = g^{z_0}, \ldots, g_n = g^{z_n}, v_1 = g^{t_1}, \ldots, v_4 = g^{t_4}, h_0 = h^{z_0}, \ldots .h_n = h^{z_n}), msk = (\alpha, t_1, t_2, t_3, t_4),$$
$$ct_{id} = (\Omega^s \cdot m, H_1(id)^s, v_1^{s-s_1}, v_2^{s_1}, v_3^{s-s_2}, v_4^{s_2})$$

The KGC can compute $(v_1^{s-s_1})^{t_2} \cdot (v_2^{s_1})^{t_1} = g^{t_1 t_2 (s-s_1)} \cdot g^{t_1 t_2 s_1} = g^{t_1 t_2 s}$. Evaluating $e(g^{t_1 t_2 s}, h^{\alpha}) = \Omega^s$ will let KGC remove the mask and find the message m. We also consider a regular IBE scheme [22]. Similar attacks are possible in some of the other standard model IBE schemes [20,2].

Waters [22]. Their construction has the following parameters,

$$params = (g, g_1 = g^{\alpha}, g_2, u', U = (u_1, \ldots, u_n)), msk = g_2^{\alpha}$$

$$ct_{id} = (m \cdot e(g_1, g_2)^t, g^t, (u \prod_{i \in \mathcal{V}} u_i)^t)$$

Similar to [17], the KGC can compute $e(g_1, g_2)^t = e(g^{\alpha}, g_2)^t = e(g^t, g_2^{\alpha})$ and get back the message. Similar attacks are also possible in other standard model IBE schemes.

Boneh-Boyen IBE [2]. The Boneh-Boyen IBE [2] has $params, msk$ and the ciphertext of m for the identity id, as defined below:

$$params = (g, X = g^x, Y = g^y), msk = (x, y), ct_{id} = (g^{s \cdot id} X^s, Y^s, e(g,g)^s \cdot m)$$

The KGC can compute $g^s = (Y^s)^{\frac{1}{y}}$, divide the last term of the ciphertext by $e(g, g^s)$ to get back the original message. We provide another vulnerable IBE scheme in Appendix B.

This vulnerability is mainly because the decryption performs a linear reconstruction of the msk. Given these identified weaknesses, we conclude that no existing IBE definitions in the standard model or blind IBE definitions capture the security of the ciphertext against the KGC. To address this issue, we propose a new IBE definition below, oblivious IBE, and subsequently provide a new IBE construction that does not suffer from the identified weaknesses.

3.2 Our Definition

Our new definition is inspired by the security definition of Emura *et al.* [8]. However, as we discussed in subsection 1.1, the KGC security definition of [8] does not allow the KGC to compute the secret key of any identity of their own. In their security definition, KGC needs to receive a message from the Certification Authority (ICA) to compute the private key. At the same time, their construction allows the KGC to compute any user's secret key. We address this issue by proposing a new KGC security game that bridges the gap between these definitions and the existing constructions. Unlike the KGC adversary of [8], our definition allows a KGC adversary to generate a secret key for any identity of their choosing.

Another major difference between our definition and the definitions of Chow [6] and Emura *et al.* [8] is the absence of the ICA. In [6,8], the identities are sent in the clear to the ICA, and the ICA generates a signature on the identity which can then be used to generate the private key. Thus, KGC and ICA need to be online to create a key. Also, if the ICA and KGC collude, then the identity/secret key pair is known to the adversary. Our model does not have this weakness as we do not employ an ICA in our definition. Another noticeable difference between the older and our new definitions is the possibility of authentication. The certification authority in older definitions can authenticate the users as the identity is sent to the ICA. Even though authentication is not possible in our definition, our proposed construction could be modified into a construction having an ICA to authenticate users. We leave the construction as future work.

We provide two security models for KGC security, namely the strong-KGC model and KGC model. Our construction is secure in the KGC model and we leave the construction of the strong-KGC model as future work. We describe our new definitions below.

Definition 1 (Oblivious Identity-Based Encryption). *An Oblivious Identity-Based Encryption defined over the identity space $\mathcal{I}$, message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ consists of the following four algorithms:*

- $\mathsf{Setup}(1^\lambda) \to (params, mpk, msk)$*: The setup algorithm takes as input a security parameter λ and outputs public parameters params, the master secret key msk and a master public key mpk.*
- $\mathsf{BlindExtract}(\mathcal{U}(params, mpk, id), \mathcal{KGC}(params, mpk, msk)) \to (sk_{id}, \perp)$*: The interactive key-issuing protocol between the user $\mathcal{U}$ and the key generation centre $\mathcal{KGC}$ generates the secret key sk_{id} for the user $\mathcal{U}'s$ identity $id \in \mathcal{I}$ and the $\mathcal{KGC}$ learns nothing.*

$\mathsf{Enc}(params, mpk, id, m) \to ct$: *The encryption algorithm takes mpk, identity* $id \in \mathcal{I}$*, the message* $m \in \mathcal{M}$ *and outputs a ciphertext* $ct \in \mathcal{C}$.

$\mathsf{Dec}(params, mpk, sk_{id}, ct) \to m$ *or* $\perp$: *The decryption algorithm takes as input* mpk, sk_{id}, ct *and outputs a message* m *or* $\perp$.

Correctness. *For all* $\lambda \in \mathbb{N}, m \in \mathcal{M}, id \in \mathcal{I}$*, we require*

$$\Pr\left[\begin{array}{c} \mathsf{Dec}(params, mpk, \\ sk_{id}, ct) = m \end{array} : \begin{array}{c} \mathsf{Setup}(1^\lambda) \to (params, mpk, msk) \\ \mathsf{BlindExtract}(\mathcal{U}(params, mpk, id), \\ \mathcal{KGC}(params, mpk, msk)) \to (sk_{id}, \perp) \\ \mathsf{Enc}(params, mpk, id, m) \to ct \end{array}\right] \geq 1 - \mathsf{negl}(\lambda).$$

Security against users. *An IBE scheme is said to be adaptively secure anonymous IBE if the advantage of the adversary* $\mathcal{A}$ *defined as* $Adv^{\textsf{Anon-IND-CPA}}_{\mathcal{IBE},\mathcal{A}}(\lambda) = |Pr[b = b'] - 1/2|$ *in the following game is negligible in the security parameter* λ. *The function* $\mathsf{CTSamp}(params, mpk)$ *takes as inputs public parameters and the master public key and outputs a random element in the ciphertext space* $\mathcal{C}$. *We define the* Anon-IND-CPA *security game below.*

- *Setup. The challenger runs* $\mathsf{Setup}(1^\lambda)$ *and sends* $(params, mpk)$ *to the adversary* $\mathcal{A}$.
- *Queries. The adversary can have two types of queries, key extraction queries that can be queried several times (q queries here) and a single challenge query in any order.*

  Key-Extraction queries: For every $i \in [q]$*, the challenger and the adversary runs the interactive key-issuing protocol* BlindExtract *with the adversary acting as the user* $\mathcal{U}$ *by providing the identity* $id_i \in \mathcal{I}$ *and the challenger providing the master secret key msk. By the end, the adversary receives secret key* sk_{id_i} *corresponding to the identity* id_i.

  Challenge. The adversary $\mathcal{A}$ *picks a message* m^* *and an identity* $id^* \neq id_i$ $\forall i \in [q]$ *and sends it to the challenger. Challenger picks a random bit* $b \leftarrow \{0, 1\}$. *If the bit* $b = 0$*, the challenger computes* $\mathsf{Enc}(params, mpk, id^*, m^*)$ *and sends it to the adversary. Otherwise, the challenger picks a random element* $C \leftarrow \mathsf{CTSamp}(params, mpk)$ *and forwards it to the adversary.*
- *Guess. Adversary outputs a guess* $b' \in \{0, 1\}$. *Adversary wins if* $b' = b$. *The advantage of the adversary is defined by*

$$Adv^{\textsf{Anon-IND-CPA}}_{\mathcal{IBE},\mathcal{A}}(\lambda) = |Pr[b = b'] - 1/2|$$

Security against KGC. *An IBE scheme is said to be* s-KGC *secure if the advantage of the adversary* $\mathcal{A}$ *defined as* $Adv^{\textsf{s-KGC}}_{\mathcal{IBE},\mathcal{A}}(\lambda) = |Pr[b = b'] - 1/2|$ *in the following game is negl. in the security parameter. The function* $\mathsf{CTSamp}(params, mpk)$ *takes as inputs public parameters and the master public key and outputs a random element in the ciphertext space* $\mathcal{C}$. *A list* IDList *is used to manage the identities queried during the* BlindExtract *phase. We define the* s-KGC *security game below.*

- *Setup. The challenger runs* $\mathsf{Setup}(1^{\lambda})$*, initializes an empty set* $\mathsf{IDList} := \phi$ *and a counter* $Q_{\mathsf{key}} := 0$*. Then, the challenger sends* $(params, mpk, msk)$ *to the adversary* $\mathcal{A}$*.*
- *Queries. The adversary can run multiple key-extraction queries* (Q_{key})*, multiple encryption queries, and a single challenge query in any order.*

  BlindExtract *queries. The challenger picks a random identity* $id \in \mathcal{I}$*, updates* $Q_{\mathsf{key}} := Q_{\mathsf{key}} + 1$ *and updates* $\mathsf{IDList}[Q_{\mathsf{key}}] = id$*. Then, the challenger and the adversary* $\mathcal{A}$ *runs the interactive key-issuing protocol with the adversary acting as the* $\mathcal{KGC}$ *and the challenger acting as the user* $\mathcal{U}$ *by providing the identity* id*.*

  Encryption queries. The adversary can submit an index $i \in [Q_{\mathsf{key}}]$ *and a message* m*. The challenger computes* $\mathsf{Enc}(params, mpk, \mathsf{IDList[i]}, m)$ *and sends it to* $\mathcal{A}$*.*

  Challenge. The adversary $\mathcal{A}$ *submits an index* $i^* \in [Q_{\mathsf{key}}]$ *and a message* m^**. The challenger sets* $id^* = \mathsf{IDList}[i^*]$ *and picks a random bit* $b \leftarrow \{0, 1\}$*. If the bit* $b = 0$*, the challenger computes* $\mathsf{Enc}(params, mpk, id^*, m^*)$ *and sends it to* $\mathcal{A}$*. Otherwise, the challenger picks a random element* $C \leftarrow \mathsf{CTSamp}(params, mpk)$ *and forwards it to the adversary.*
- *Guess. The adversary outputs a guess* $b' \in \{0, 1\}$*.* $\mathcal{A}$ *wins if* $b' = b$*. The advantage of the adversary is defined by*

$$Adv^{\textsf{s-KGC}}_{\mathcal{IBE},\mathcal{A}}(\lambda) = |Pr[b = b'] - 1/2|$$

We call an IBE scheme strong-Oblivious Identity-Based Encryption(s-OIBE) if it is both Anon-IND-CPA *secure and* s-KGC *secure. In this work, we consider a weaker security game* KGC *where the adversary cannot have encryption queries. An IBE scheme that is* Anon-IND-CPA *secure and* KGC *secure is called Oblivious Identity-Based Encryption(OIBE) and we provide a construction for OIBE. We leave the construction for s-OIBE as future work.*

4 Construction

We provide our construction of Oblivious IBE based on Wee's IBE scheme [23] using the techniques from the oblivious Pseudo-Fandom Function by Jarecki and Liu [19].

4.1 Our Construction

Let N be the product of two distinct primes of length $\Theta(\lambda)$ and $BG(1^{\lambda})$ takes as input a security parameter λ and outputs $(e, g_1, h_1, N, G, H, G_T)$ as described in subsection 2.1. Let $\mathsf{HE} = (\mathsf{HE.Primes}, \mathsf{HE.Setup}, \mathsf{HE.KeyGen}, \mathsf{HE.Enc}, \mathsf{HE.Dec})$ be an additive homomorphic encryption scheme with message space defined over $\mathbb{Z}_N$ and $\mathsf{H} : G_T \to \{0, 1\}^{\lambda}$ is drawn from a family of pairwise independent hash functions. The underlying proof system PoK is considered zero-knowledge and simulation extractable. We should note that the Setup functionality should be run by a trusted party since the knowledge of the primes p_1 and p_2 would allow an adversarial KGC to break the sub-group decision assumption. We provide our construction in Fig. 2

4.2 Correctness and Security

Correctness. The correctness of the scheme follows from the following observations:

$$\forall id \in \mathcal{I},\ sk = h^{\sigma_{val}} \cdot val = h^{\frac{v}{\alpha+id}} = u^{\frac{1}{\alpha+id}}.$$
$$\forall m \in \mathcal{M},\ ct_1 \oplus \mathsf{H}(e(ct_0, sk_{id})) = \mathsf{H}(e(g_1,u)^s) \oplus m \oplus \mathsf{H}(e(g_1^{(\alpha+id)s}, u^{\frac{1}{\alpha+id}})) = m\cdot$$

Security against users.

Theorem 1. *Assuming the hardness of the sub-group decision assumption in groups G and H, a semantically secure homomorphic encryption scheme on $\mathbb{Z}_N$ which satisfies properties in sub-section 2.2, and assuming the proof of knowledge system in equation 1 is zero-knowledge and simulation extractable, the IBE scheme in Fig. 2 is secure against* Anon-IND-CPA *game.*

Proof. We proceed through a series of games. Although the proof is similar to the proof of [23], we have to modify it for our construction due to the additional leakage in the master public key mpk. We address this leakage by modifying an information-theoretic lemma which is the core of the work of [23]. We show that there exist adversaries $\mathcal{A}'_1, \mathcal{A}'_2, \mathcal{A}'_3$ such that

$$Adv^{\mathsf{Anon\text{-}IND\text{-}ID\text{-}CPA}}_{\mathcal{IBE},\mathcal{A}} \leq Adv^{SD_1}_{\mathcal{G},\mathcal{A}'_1} + Adv^{\mathsf{HE}}_{\mathcal{A}'_2} + (q+2)\cdot Adv^{SD_2}_{\mathcal{G},\mathcal{A}'_3} + \frac{(q+2)^2}{p_2} + \frac{1}{p_2} + 2^{-\lambda}.$$

For the homomorphic encryption and decision sub-group assumption reductions, the challenger has to not only provide the parameters corresponding to that particular assumption but also has to generate and send the parameters of other primitives too *i.e.* a homomorphic encryption semantic security challenger has to generate and send a bilinear map to the adversary. This is because the adversary cannot generate the bilinear map on its own without the knowledge of the primes (p_1, p_2). These modifications do not affect the security as the homomorphic encryption and bilinear map are on different groups.
The advantage of an adversary in Game i is denoted by Adv_i and the advantage of an adversary in sub-game Sub-Game i.j.k is given by $Adv_{i.j.k}$. The proofs of the lemmas are provided in Appendix C. we describe the games below.

Game 0. We define the first game Game 0 to be the Anon-IND-CPA security game. The challenger uses the simulation extractable property of the underlying zero-knowledge proof to extract the identities from the adversary $\mathcal{A}$ during the BlindExtract queries similar to Jarecki *et.al*[19]. The description of Game 0 is provided below.

```
$\mathsf{Setup}(1^\lambda)$ :
    $(p_1, p_2) \leftarrow \mathsf{HE.Primes}(1^\lambda)$.
    $par_1 := (g, N) \leftarrow \mathsf{HE.Setup}(p_1, p_2)$.
    $par_2 := (e, g_1, h_1, N, G, H, G_T) \leftarrow BG(p_1, p_2)$.
    $params := (par_1, par_2, \mathsf{H})$.
    $(pk_{\mathcal{KGC}}, sk_{\mathcal{KGC}}) \leftarrow \mathsf{HE.KeyGen}(g, N)$.
    $\alpha \leftarrow \mathbb{Z}_N, C_\alpha := \mathsf{HE.Enc}(pk_{\mathcal{KGC}}, \alpha)$.
    $h \leftarrow H_{p_1}, v \leftarrow \mathbb{Z}_N,$ set $u := h^v$.
    $msk := (\alpha, v, u, sk_{\mathcal{KGC}})$.
    $mpk := (g_1, g_1^\alpha, e(g_1, u), h, pk_{\mathcal{KGC}}, C_\alpha)$.
```

```
$\mathsf{Enc}(params, mpk, id \in \mathcal{I}, m \in \mathcal{M})$ :
    Picks $\leftarrow \mathbb{Z}_N$.
    $ct_0 = g_1^{(\alpha+id)s}$.
    $ct_1 = \mathsf{H}(e(g_1, u)^s) \oplus m$.
    return $(ct_0, ct_1)$.

$\mathsf{Dec}(params, mpk, sk_{id}, ct)$ :
    Parse $ct$ as $(ct_0, ct_1)$.
    return $ct_1 \oplus \mathsf{H}(e(ct_0, sk_{id}))$.
```

```
$\mathsf{BlindExtract}$
$\mathcal{U}(params, mpk, id)$                                          $\mathcal{KGC}(params, mpk, msk)$
Parse $params, mpk$ as
$params = (g, N, e, g_1, h_1, G, H, G_T, \mathsf{H})$.
$mpk = (g_1, g_1^\alpha, e(g, u), h, pk_{\mathcal{KGC}}, C_\alpha)$.
$(pk_u, sk_u) \leftarrow \mathsf{HE.KeyGen}(g, N)$.
$a \leftarrow \mathbb{Z}_N, C_a := \mathsf{HE.Enc}(pk_u, a)$.
$C_{id} := (C_\alpha \cdot \mathsf{HE.Enc}(pk_{\mathcal{KGC}}, id))^a$ .
$\pi := \mathsf{PoK}\{id| \quad \exists a \in \mathbb{Z}_N,$ s.t.
    $C_a = \mathsf{HE.Enc}(pk_u, a) \wedge$
    $C_{id} \in (C_\alpha \cdot \mathsf{HE.Enc}(pk_{\mathcal{KGC}}, id))^a\}$.
                        $\xrightarrow{(pk_u, C_a, C_{id}, \pi)}$
                                                                        Abort if $\pi$ does not verify.
                                                                        $\beta := \mathsf{HE.Dec}(sk_{\mathcal{KGC}}, C_{id})$.
                                                                        if $\gcd(N, \beta) \neq 1,$ abort.
                                                                        $\gamma := \beta^{-1} \mod N$.
                                                                        $\sigma_u \leftarrow \mathbb{Z}_N, val := h^{\sigma_u}$.
                                                                        $C_{sk} := C_a^{v\gamma} \cdot \mathsf{HE.Enc}(pk_u, -\sigma_u)$.
                        $\xleftarrow{(C_{sk}, val)}$
$\sigma_{val} \leftarrow \mathsf{HE.Dec}(sk_u, C_{sk})$.
$sk := h^{\sigma_{val}} \cdot val$.
```

Fig. 2. Oblivious IBE Construction with identity space $\mathcal{I} = \mathbb{Z}_N$ and message space $\mathcal{M}$

1. The challenger $\mathcal{C}$ runs the $\mathsf{Setup}(\lambda)$ and sends $params = (par_1, par_2, \mathsf{H}) = (g, N, e, g_1, h_1, G, H, G_T, \mathsf{H})$, $mpk = (g_1, g_1^{\alpha}, e(g_1, u), h, pk_{\mathsf{KGC}}, C_{\alpha})$ to the adversary $\mathcal{A}$.
2. $\mathcal{A}$ and $\mathcal{C}$ run the $\mathsf{BlindExtract}$ protocol q times with the identities $id_1, \ldots,$ id_q and a single challenge query in any order:
   (a) For $i \in [q]$,
      i. $\mathcal{A}$ generates $(pk_{u_i}, sk_{u_i}) \leftarrow \mathsf{HE.KeyGen}(g, N)$. Sample $a_i \leftarrow \mathbb{Z}_N$, compute $C_{a_i} := \mathsf{HE.Enc}(pk_{u_i}, a_i)$, $C_{id_i} = (C_{\alpha} \cdot \mathsf{HE.Enc}(pk_{\mathsf{KGC}}, id_i))^{a_i}$, $\pi_i = \mathsf{PoK}\{id_i | \exists a_i \in \mathbb{Z}_N, \text{s.t. } C_{a_i} = \mathsf{HE.Enc}(pk_{u_i}, a_i)$ and $C_{id_i} \in (C_{\alpha} \cdot \mathsf{HE.Enc}(pk_{\mathcal{KGC}}, id_i))^{a_i})\}$ and send $(pk_{u_i}, C_{a_i}, C_{id_i}, \pi_i)$ to $\mathcal{C}$.
      ii. $\mathcal{C}$ verifies the proof π_i, and aborts if it does not verify. Otherwise, $\mathcal{C}$ extracts id_i from π_i and compute $\beta_i := \mathsf{HE.Dec}(sk_{\mathcal{KGC}}, C_{id_i})$. Aborts if $gcd(\beta_i, N) \neq 1$. Otherwise, compute $\gamma_i := \beta_i^{-1} \bmod N$. Sample $\sigma_{u_i} \leftarrow \mathbb{Z}_N$ and compute $C_{sk_i} := C_{a_i}^{\gamma_i v} \cdot \mathsf{HE.Enc}(pk_{u_i}, -\sigma_{u_i})$, $val_i := h^{\sigma_{u_i}}$. Finally, sends (C_{sk_i}, val_i) to $\mathcal{A}$.
   (b) $\mathcal{A}$ picks a message m^* and identity $id^* \neq id_i\ \forall i \in [q]$ from the identity space $\mathcal{I}$ and sends (m^*, id^*) to $\mathcal{C}$.
3. $\mathcal{C}$ picks a bit $b \in \{0, 1\}$. If the bit $b = 0$, $\mathcal{C}$ sends $C_0 = (g_1^{(\alpha + id^*)s}, \mathsf{H}(e(g_1, u)^s)$ $\oplus m^*)$. Else, send $C_1 \leftarrow \mathsf{CTSamp}(params, mpk)$ to $\mathcal{A}$.
4. $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$.

Game 1. We define $\mathsf{Game\ 1}$ similar to $\mathsf{Game\ 0}$ with some additional assumptions.

- We never come across an identity id such that $id = \alpha \mod p_1$. This would result in solving the discrete algorithm of g_1^{α}.
- The adversary's queries $id_1, id_2 \ldots, id_q, id^* \in \mathbb{Z}_N$ are distinct.
- $id_1, \ldots, id_q, id^*$ are distinct mod p_2, otherwise, $gcd(id_i - id_j, N)$ could be used to factor N.

The challenger aborts if any of the above conditions are met. We will evaluate the probabilities of these events later in the proof. Thus, $Adv_0 \approx Adv_1$.

Game 2. We set $C_{sk_i} := \mathsf{HE.Enc}(pk_{u_i}, \sigma_{v_i}), val_i := h^{\frac{v}{\alpha + id_i} - \sigma_{v_i}}\ \forall i \in [q]$ where $\sigma_{v_i} \leftarrow \mathbb{Z}_N$ and $\sigma_{u_i} = \frac{v}{\alpha + id_i} - \sigma_{v_i}$. As these modifications are only notational, $Adv_1 \approx Adv_2$.

Game 3. The ciphertext C_0 is set to be $C_0 := (C, H(e(C, sk_{id^*}) \oplus m^*))$ where $C \leftarrow G_{p_1}$. For any id^*, $e(g_1, u)^s = e(g_1^{(\alpha + id^*)s}, u^{\frac{1}{\alpha + id^*}}) = e(g_1^{(\alpha + id^*)s},$ $sk_{id^*})$. If $\alpha + id^* \neq 0$, then C and $g_1^{(\alpha + id^*)s}$ are identically distributed. Thus, $Adv_2 \approx Adv_3$.

Game 4. We change the distribution of C in C_0 from $C \leftarrow G_{p_1}$ to $C \leftarrow G_{p_1} G_{p_2}$.

Lemma 1. *Assuming the subgroup decision assumption SD_1 in group G, $Adv_3 - Adv_4 \leq Adv_{\mathcal{A}'_1}^{SD_1, G}$.*

Game 5. We set $C_{\alpha} := \mathsf{HE.Enc}(pk_{\mathcal{KGC}}, \alpha')$, where $\alpha' \leftarrow \mathbb{Z}_N$ in this security game.

Lemma 2. *$Adv_4 - Adv_5 \leq Adv_{\mathcal{A}'_2}^{\mathsf{HE}}$ where $Adv_{\mathcal{A}'_2}^{\mathsf{HE}}$ is the advantage of an adversary against semantic security of the underlying homomorphic encryption scheme* HE.

Game 6. We make the following modifications in Game 6. Sample $r_1, r_2, \ldots, r_{q+2}$, $\alpha_1, \ldots, \alpha_{q+2} \leftarrow \mathbb{Z}_N$.

$$mpk := (g_1, g_1^{\alpha}, e(g_1, uh_2^{vr_1+\cdots+vr_{q+2}}), hh_2^{r_1+\cdots+r_{q+2}}, pk_{\mathsf{KGC}}, C_\alpha)$$

$$\text{For all } i \in [q], val_i := h^{\frac{v}{\alpha+id_i}-\sigma_{v_i}} h_2^{r_1\left(\frac{v}{\alpha_1+id_i}-\sigma_{v_i}\right)+\cdots+r_{q+2}\left(\frac{v}{\alpha_{q+2}+id_i}-\sigma_{v_i}\right)}$$

$$sk_{id^*} := h^{\frac{v}{\alpha+id^*}} h_2^{\frac{vr_1}{\alpha_1+id^*}+\cdots+\frac{vr_{q+2}}{\alpha_{q+2}+id^*}}$$

Lemma 3. $Adv_5 - Adv_6 \leq (q+2) \cdot Adv_{\mathcal{A}'_3}^{SD_2,H}$.

Game 7. Sample $t_0, \ldots, t_{q+1} \leftarrow \mathbb{Z}_{p_2}$. We replace the following values:

$$mpk := (g_1, g_1^{\alpha}, e(g_1, uh_2^{vt_0}), hh_2^{t_0}, pk_{\mathsf{KGC}}, C_\alpha)$$

$$\text{For all } i \in [q], val_i := h^{\frac{v}{\alpha+id_i}-\sigma_{v_i}} h_2^{t_i}$$

$$sk_{id^*} := h^{\frac{v}{\alpha+id^*}} h_2^{t_{q+1}}$$

Lemma 4. $Adv_6 - Adv_7 \leq \frac{(q+2)^2}{p_2}$.

The game Game 7 is statistically close to Game 6. For ease of notation, we consider the challenge to be queried after all the key-extraction queries. The proof holds even if the order of the queries is different. The H_{p_2} components of $hh_2^{r_1+\cdots+r_{q+2}}$, val_i and sk_{id^*} in their logarithms w.r.t h_2 are

$$\underbrace{\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \frac{v}{\alpha_1+id_1} - \sigma_{v_1} & \frac{v}{\alpha_1+id_1} - \sigma_{v_1} & \cdots & \frac{v}{\alpha_{q+2}+id_1} - \sigma_{v_1} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{v}{\alpha_1+id_q} - \sigma_{v_q} & \frac{v}{\alpha_1+id_q} - \sigma_{v_q} & \cdots & \frac{v}{\alpha_{q+2}+id_q} - \sigma_{v_q} \\ \frac{v}{\alpha_1+id^*} & \frac{v}{\alpha_1+id^*} & \cdots & \frac{v}{\alpha_{q+2}+id^*} \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_{q+1} \\ r_{q+2} \end{pmatrix}}_{R} = \underbrace{\begin{pmatrix} t'_0 \\ t'_1 \\ \vdots \\ t'_q \\ t'_{q+1} \end{pmatrix}}_{T}.$$

After applying the elementary row operations on A, we get $\det(A) = v^{q+1} \det(B) \bmod p_2$, where

$$B = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \frac{1}{\alpha_1+id_1} & \frac{1}{\alpha_1+id_1} & \cdots & \frac{1}{\alpha_{q+2}+id_1} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{\alpha_1+id_q} & \frac{1}{\alpha_1+id_q} & \cdots & \frac{1}{\alpha_{q+2}+id_q} \\ \frac{1}{\alpha_1+id^*} & \frac{1}{\alpha_1+id^*} & \cdots & \frac{1}{\alpha_{q+2}+id^*} \end{pmatrix}.$$

In the following lemma, we represent id^* as id_{q+1}.

Lemma 5.

$$\det(B) = \delta \cdot \frac{\prod_{1 \le i < j \le q+1} (id_i - id_j) \prod_{1 \le i < j \le q+2} (\alpha_i - \alpha_j)}{\prod_{i=1}^{q+2} \prod_{j=1}^{q+1} (\alpha_i + id_j)} \text{ for a constant } \delta \in \mathbb{Z}_{p_2}^{*} \cdot$$

The determinant of the matrix $\det(B) \neq 0 \mod p_2$ whenever id_i, id^* and α_i are distinct $\mod p_2$ and $\alpha_i + id_j \neq 0$. This happens with probability greater than $1 - \frac{(q+2)^2}{p_2}$. This would mean that there exists a one-to-one correspondence between the two matrices R and T. So, as long as the values in R are chosen uniformly at random, the values in T are uniformly random over $\mathbb{Z}_{p_2}^{q+2}$. Thus, we can replace T with elements in $\mathbb{Z}_{p_2}^{q+2}$ chosen uniformly at random.

Game 8. In this game, the challenge ciphertext is generated as

$$C_0 := (C, m') \text{ where } C \leftarrow G_{p_1} G_{p_2} \text{ and } m' \leftarrow \mathcal{M} \cdot$$

Lemma 6. $Adv_7 - Adv_8 \le \frac{1}{p_2} + 2^{-\lambda}$.

Observe that after the modifications in Game 7, we have

$$\mathsf{H}(e(C, sk_{id^*})) = \mathsf{H}(e(C, h^{\frac{v}{\alpha + id^*}}) \cdot e(C, h_2^{t_{q+1}})) \cdot$$

As t_{q+1} is independent of all the other values, the term $e(C, h_2^{t_{q+1}})$ has a min-entropy of $\log(p_2)$ as long as C has a non-trivial component in G_{p_2} . H is a universal hash function and the Leftover Hash Lemma ensures that $\mathsf{H}(e(C, sk_{id^*}))$ is $2^{-\lambda}$ close to the uniform distribution.

$$Adv_7 - Adv_8 \le \frac{1}{p_2} + 2^{-\lambda}.$$

Since C_0 in Game 8 is independent of m^* and id^*, the view of the adversary $\mathcal{A}$ in Game 8 is statistically independent of the challenge bit b. Thus, $Adv_8 = 0$. Combining all the previous lemmas, we have

$$Adv_0 \le Adv_{\mathcal{G},\mathcal{A}_1'}^{SD_1} + Adv_{\mathcal{A}_2'}^{\mathsf{HE}} + (q+2) \cdot Adv_{\mathcal{G},\mathcal{A}_3'}^{SD_2} + \frac{(q+2)^2}{p_2} + \frac{1}{p_2} + 2^{-\lambda}.$$

□

Security against KGC.

Theorem 2. *Assuming the hardness of the sub-group decision assumption in groups G and H, a semantically secure homomorphic encryption scheme on $\mathbb{Z}_N$ which satisfies properties in sub-section 2.2, and assuming the proof of knowledge system in equation 1 is zero-knowledge and simulation extractable, the IBE scheme in Fig. 2 is secure against KGC game.*

Proof. We borrow techniques from Wee [23] to prove the above theorem. However, a major difference between proof of [23] and ours is that the KGC is given msk in our KGC security game. We carefully modify the proof to address this additional leakage. Similar to our user security proof, the challenger used in the reductions has to provide public parameters of other assumptions. This does not affect the security as the assumptions are considered in different groups. We show that there exist adversaries $\mathcal{A}'_1, \mathcal{A}'_2, \mathcal{A}'_3$ such that

$$Adv^{\mathsf{KGC}}_{\mathcal{IBE},\mathcal{A}} \leq q \cdot Adv^{\mathsf{HE}}_{\mathcal{A}'_1} + Adv^{SD_1}_{\mathcal{G},\mathcal{A}'_2} + 2 \cdot Adv^{SD_2}_{\mathcal{G},\mathcal{A}'_3} + \frac{1}{p_2} + 2^{-\lambda}.$$

We proceed through a series of games. The $\mathsf{Game\ 0}$ is the KGC security game. The advantage of an adversary in $\mathsf{Game\ i}$ is denoted by Adv_i and the advantage of an adversary in sub-game $\mathsf{Sub\text{-}Game\ i.j}$ is given by $Adv_{i.j}$. Let q be the total number of $\mathsf{BlindExtract}$ queries in the security game. The proofs of the lemmas are provided in Appendix C.

Game 0. Our KGC security game is described below.

1. The challenger $\mathcal{C}$ runs $\mathsf{Setup}(1^\lambda)$, initializes an empty set $\mathsf{IDList} := \phi$. Then, the challenger sends $params = (par_1, par_2, \mathsf{H}) = (g, N, e, g_1, h_1, N, G, H, G_T, \mathsf{H})$, $mpk := (g_1, g_1^\alpha, e(g_1, u), h, pk_{\mathcal{KGC}}, C_\alpha), msk := (\alpha, v, u, sk_{\mathcal{KGC}})$ to the adversary $\mathcal{A}$.
2. $\mathcal{C}$ and $\mathcal{A}$ runs the $\mathsf{BlindExtract}$ protocol and a single challenge query:
   (a) When the adversary submits i^{th} $\mathsf{BlindExtract}$ query, where $i \in [q]$
      i. $\mathcal{C}$ samples an identity $id_i \leftarrow \mathbb{Z}_N$, and updates $\mathsf{IDList}[i] := id_i$. The challenger samples $a_i \leftarrow \mathbb{Z}_N$ and generates the public key/secret key pair $(pk_{u_i}, sk_{u_i}) \leftarrow \mathsf{HE.KeyGen}(g, N)$. Then, $\mathcal{C}$ computes $C_{a_i} := \mathsf{HE.Enc}(pk_u, a_i)$, $C_{id_i} = (C_\alpha \cdot \mathsf{HE.Enc}(pk_{\mathcal{KGC}}, id_i))^{a_i}$. The challenger also computes a proof of knowledge $\pi_i := \mathsf{PoK}\{id_i | \exists a_i \in \mathbb{Z}_N, \text{s.t. } C_{a_i} = \mathsf{HE.Enc}(pk_{u_i}, a_i) \wedge C_{id_i} \in (C_\alpha \cdot \mathsf{HE.Enc}(pk_{\mathcal{KGC}}, id_i))^{a_i})\}$ and sends $(pk_{u_i}, C_{a_i}, C_{id_i}, \pi_i)$ to $\mathcal{A}$.
      ii. $\mathcal{A}$ verifies the proof, computes $\beta_i := a_i(\alpha + id_i)$, $\gamma_i := \beta_i^{-1} \bmod N$, samples $\sigma_{u_i} \leftarrow \mathbb{Z}_N$ $C_{sk_i} := C_{a_i}^{\gamma_i v} \cdot \mathsf{HE.Enc}(pk_{u_i}, -\sigma_{u_i})$ and sends $(C_{sk_i}, val_i := h^{\sigma_{u_i}})$ to $\mathcal{C}$.
   (b) $\mathcal{A}$ picks an index $i^* \in [q]$ and a message $m^* \in \mathcal{M}$ and sends it to $\mathcal{C}$.
3. On receiving the index $i^* \in [q]$ and message m^* from the adversary, if i^*-th $\mathsf{BlindExtract}$ query was already queried, $\mathcal{C}$ sets $id^* = \mathsf{IDList}[i^*]$, sample $b \leftarrow \{0, 1\}$. Computes $C_0 = (g_1^{(\alpha+id^*)s}, \mathsf{H}(e(g, u)^s) \oplus m^*)$ and $C_1 \leftarrow \mathsf{CTSamp}(params, mpk)$ and sends C_b to $\mathcal{A}$.
4. Adversary outputs a guess $b' \in \{0, 1\}$.

The advantage of the adversary in the above game is defined by $Adv_0 = Pr[b = b']$.

Game 1. This game is the same as $\mathsf{Game\ 0}$ except that instead of PoK, the proofs π_i are simulated by the simulator $\mathsf{Sim} = (Sim_1, Sim_2)$. We modify PoK to $r \leftarrow Sim_1(1^\lambda)$ and proof $\pi_i = Sim_2(r, params, mpk, pk_{u_i})$ $\forall i \in [q]$.

Lemma 7. *Assuming the existence of a proof of knowledge system that is zero-knowledge and simulation extractable,* $Adv_0 - Adv_1 \leq q \cdot negl(\lambda)$.

Game 2. In this game, for all $i \in [q]$, C_{a_i} is replaced with $C_{a_i} := \mathsf{HE.Enc}(pk_u, {a_i}')$ where $a_i' \leftarrow \mathbb{Z}_N$. The security follows from the semantic security of the homomorphic encryption scheme.

Lemma 8. *$Adv_1 - Adv_2 \leq q \cdot Adv^{\mathsf{HE}}_{\mathcal{A}_1'}$.*

Game 3. We replace C_{id_i} with $C_{id_i} = \mathsf{HE.Enc}(pk_{\mathcal{KGC}}, r_i')$ $\forall i \in [q]$ where $r_i' \leftarrow \mathbb{Z}_N$. In the previous games, a_i was hiding the identity id_i in C_{id_i}. Replacing a_i with random a_i' in Game 2 game allows us to make this modification. Thus, $Adv_2 \approx Adv_3$.

Game 4. We modify the challenge ciphertext C_0 in this game. The challenger samples $C \leftarrow G_{p_1}$ and computes $C_0 = (C, H(e(C, sk_{id^*}) \oplus m^*))$. This follows from the observation that (1) $e(g_1, u)^s = e(g_1^{(\alpha+id^*)s}, u^{\frac{1}{\alpha+id^*}}) = e(g_1^{(\alpha+id^*)s}, sk_{id^*})$ and (2) $g_1^{(\alpha+id^*)s}$ and $C \leftarrow G_{p_1}$ are identically distributed whenever $\alpha + id^* \neq 0$. Thus, $Adv_3 \approx Adv_4$.

Game 5. We change the distribution of C in C_0 from $C \leftarrow G_{p_1}$ to $C \leftarrow G_{p_1}G_{p_2}$. We use the subgroup decision assumption to justify this modification.

Lemma 9. *$Adv_4 - Adv_5 \leq Adv^{SD_1,G}_{\mathcal{A}_2'}$.*

Game 6. We modify the following values in this game. Sample $r_1, r_2 \leftarrow \mathbb{Z}_N$, $id_a, id_b \leftarrow \mathcal{I}$.

$$mpk := (g_1, g_1^{\alpha}, e(g_1, h^v h_2^{v(r_1+r_2)}), hh_2^{r_1+r_2}, pk_{\mathcal{KGC}}, C_\alpha)\cdot$$

$$msk := (\alpha, v, h^v h_2^{v(r_1+r_2)}, sk_{\mathcal{KGC}})\cdot$$

$$sk_{id^*} := h^{\frac{v}{\alpha+id^*}} h_2^{r_1 \frac{v}{\alpha+id_a} + r_2 \frac{v}{\alpha+id_b}}.$$

We show that Game 5 and Game 6 are computationally close through a series of sub-games.

Lemma 10. *$Adv_5 - Adv_6 \leq 2 \cdot Adv^{SD_2,H}_{\mathcal{A}_3'}$.*

Game 7. We replace the following values, sample $t_0, t_1 \leftarrow \mathbb{Z}_N$,

$$mpk := (g_1, g_1^{\alpha}, e(g_1, h^v h_2^{vt_0}), hh_2^{t_0}, pk_{\mathcal{KGC}}, C_\alpha)\cdot$$

$$msk := (\alpha, v, h^v h_2^{vt_0}, sk_{\mathcal{KGC}})\cdot$$

$$sk_{id^*} := h^{\frac{v}{\alpha+id^*}} h_2^{t_1}\cdot$$

Lemma 11. *$Adv_6 \approx Adv_7$.*

The game Game 7 is statistically close to Game 6. The H_{p_2} components of sk_{id^*} in their logarithms w.r.t h_2 are

$$\underbrace{\begin{pmatrix} 1 & 1 \\ \frac{v}{\alpha+id_a} & \frac{v}{\alpha+id_b} \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} r_1 \\ r_2 \end{pmatrix}}_{R} = \underbrace{\begin{pmatrix} t_0' \\ t_1' \end{pmatrix}}_{T}.$$

When $id_a \neq id_b$, $\alpha + id_a \neq 0$ and $\alpha + id_b \neq 0$, then $\det(A) \neq 0$ and this happens with probability $\geq 1 - negl(\lambda)$. Thus, with high probability, there is a one-to-one correspondence between R and T. Thus we can replace t'_0 and t'_1 with values t_0 and t_1 chosen uniformly at random.

Game 8. In this game, the challenge ciphertext C_0 is generated as

$$C_0 := (C, m') \text{ where } C \leftarrow G_{p_1} G_{p_2} \text{ and } m' \leftarrow \mathcal{M}.$$

Lemma 12. $Adv_7 - Adv_8 \leq \frac{1}{p_2} + 2^{-\lambda}$.

Observe that after the modifications in Game 7, we have

$$\mathsf{H}(e(C, sk_{id^*})) = \mathsf{H}(e(C, h^{\frac{v}{\alpha + id^*}}) \cdot e(C, h_2^{t_1})).$$

As t_1 is independent of all the other values, the term $e(C, h_2^{t_1})$ has a min-entropy of $\log(p_2)$ as long as C has a non-trivial component in G_{p_2} . H is a universal hash function and the Leftover Hash Lemma ensures that $\mathsf{H}(e(C, sk_{id^*}))$ is $2^{-\lambda}$ close to the uniform distribution. Thus,

$$Adv_7 - Adv_8 \leq \frac{1}{p_2} + 2^{-\lambda}.$$

Since C_0 in Game 8 is independent of m^* and id^*, the view of the adversary $\mathcal{A}$ in Game 8 is statistically independent of the challenge bit b. Thus, $Adv_8 = 0$. Combining all the previous lemmas and lemmas, we have

$$Adv_0 \leq q \cdot Adv_{\mathcal{A}'_1}^{\mathsf{HE}} + Adv_{\mathcal{G},\mathcal{A}'_2}^{SD_1} + 2 \cdot Adv_{\mathcal{G},\mathcal{A}'_3}^{SD_2} + \frac{1}{p_2} + 2^{-\lambda}.$$

□

5 Conclusion

Identity-based encryption is a useful cryptographic primitive that can relieve us from the cost of managing a PKI. One of the main concerns that prevent the wide adoption of IBE is the key escrow problem. In this paper, we revisit this concern and investigate how we may resolve it without relying on a trusted party (*i.e.,* an identity certifying authority (ICA) that was employed in previous work [6,8,9]) and without relying on the random oracle model. After pointing out vulnerabilities of multiple existing IBE schemes against an adversarial KGC, we introduce a new definition for an oblivious IBE that allow users to ask the KGC for a secret key on an identity without leaking any information about the identity to the KGC. Furthermore, we propose a novel oblivious IBE construction based on combining Wee's IBE [23] and Jarecki and Liu's OPRF [19] that is provably secure against an adversarial KGC and corrupted users while also providing high efficiency guarantees.

References

1. Al-Riyami, S.S., Paterson, K.G.: Certificateless public key cryptography. In: Laih, C. (ed.) Advances in Cryptology - ASIACRYPT 2003, 9th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, November 30 - December 4, 2003, Proceedings. Lecture Notes in Computer Science, vol. 2894, pp. 452–473. Springer (2003). https://doi.org/10.1007/978-3-540-40061-5_29
2. Boneh, D., Boyen, X.: Efficient selective identity-based encryption without random oracles. J. Cryptol. **24**(4), 659–693 (Oct 2011). https://doi.org/10.1007/s00145-010-9078-6
3. Boneh, D., Franklin, M.K.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings. Lecture Notes in Computer Science, vol. 2139, pp. 213–229. Springer (2001). https://doi.org/10.1007/3-540-44647-8_13
4. Camenisch, J., Kohlweiss, M., Rial, A., Sheedy, C.: Blind and anonymous identity-based encryption and authorised private searches on public key encrypted data. In: Jarecki, S., Tsudik, G. (eds.) Public Key Cryptography – PKC 2009. p. 196–214. Springer Berlin Heidelberg, Berlin, Heidelberg (2009)
5. Camenisch, J., Shoup, V.: Practical verifiable encryption and decryption of discrete logarithms. In: Boneh, D. (ed.) Advances in Cryptology - CRYPTO 2003. LNCS, vol. 2729, pp. 126–144. Springer Berlin Heidelberg, Berlin, Heidelberg (2003)
6. Chow, S.S.M.: Removing escrow from identity-based encryption. In: Jarecki, S., Tsudik, G. (eds.) Public Key Cryptography - PKC 2009, 12th International Conference on Practice and Theory in Public Key Cryptography, Irvine, CA, USA, March 18-20, 2009. Proceedings. Lecture Notes in Computer Science, vol. 5443, pp. 256–276. Springer (2009). https://doi.org/10.1007/978-3-642-00468-1_15
7. Dodis, Y., Yampolskiy, A.: A verifiable random function with short proofs and keys. In: Vaudenay, S. (ed.) Public Key Cryptography - PKC 2005. LNSC, vol. 3386, pp. 416–431. Springer Berlin Heidelberg, Berlin, Heidelberg (2005)
8. Emura, K., Katsumata, S., Watanabe, Y.: Identity-based encryption with security against the KGC: A formal model and its instantiation from lattices. In: Sako, K., Schneider, S.A., Ryan, P.Y.A. (eds.) Computer Security - ESORICS 2019 - 24th European Symposium on Research in Computer Security, Luxembourg, September 23-27, 2019, Proceedings, Part II. Lecture Notes in Computer Science, vol. 11736, pp. 113–133. Springer (2019). https://doi.org/10.1007/978-3-030-29962-0_6
9. Emura, K., Katsumata, S., Watanabe, Y.: Identity-based encryption with security against the KGC: A formal model and its instantiations. Theor. Comput. Sci. **900**, 97–119 (2022). https://doi.org/10.1016/j.tcs.2021.11.021
10. Garg, S., Hajiabadi, M., Mahmoody, M., Rahimi, A.: Registration-based encryption: Removing private-key generator from ibe. In: Beimel, A., Dziembowski, S. (eds.) Theory of Cryptography. p. 689–718. Springer International Publishing, Cham (2018)
11. Garg, S., Hajiabadi, M., Mahmoody, M., Rahimi, A., Sekar, S.: Registration-based encryption from standard assumptions. In: Lin, D., Sako, K. (eds.) Public-Key Cryptography - PKC 2019 - 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography, Beijing, China, April 14-17, 2019, Proceedings, Part II. Lecture Notes in Computer Science, vol. 11443, pp. 63–93. Springer (2019). https://doi.org/10.1007/978-3-030-17259-6_3

12. Garg, S., Hajiabadi, M., Mahmoody, M., Rahimi, A., Sekar, S.: Registration-based encryption from standard assumptions. In: Lin, D., Sako, K. (eds.) Public-Key Cryptography – PKC 2019. p. 63–93. Springer International Publishing, Cham (2019)
13. Glaeser, N., Kolonelos, D., Malavolta, G., Rahimi, A.: Efficient registration-based encryption. Cryptology ePrint Archive, Paper 2022/1505 (2022). https://doi.org/10.1145/3576915.3616596, https://eprint.iacr.org/2022/1505
14. Gong, J., Libert, B., Ramanna, S.C.: Compact IBBE and Fuzzy IBE from Simple Assumptions. In: SCN 2018 - 11th Conference on Security and Cryptography for Networks. pp. 1–29. Security and Cryptography for Networks (SCN) 2018, Amalfi, Italy (Sep 2018), https://hal.inria.fr/hal-01686690
15. Goyal, R., Vusirikala, S.: Verifiable registration-based encryption. In: Micciancio, D., Ristenpart, T. (eds.) Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part I. Lecture Notes in Computer Science, vol. 12170, pp. 621–651. Springer (2020). https://doi.org/10.1007/978-3-030-56784-2_21
16. Goyal, V.: Reducing trust in the pkg in identity based cryptosystems. In: Menezes, A. (ed.) Advances in Cryptology - CRYPTO 2007. p. 430–447. Springer Berlin Heidelberg, Berlin, Heidelberg (2007)
17. Green, M., Hohenberger, S.: Blind identity-based encryption and simulatable oblivious transfer. In: Kurosawa, K. (ed.) Advances in Cryptology – ASIACRYPT 2007. p. 265–282. Springer Berlin Heidelberg, Berlin, Heidelberg (2007)
18. Izabachène, M., Pointcheval, D.: New anonymity notions for identity-based encryption. In: Ostrovsky, R., Prisco, R.D., Visconti, I. (eds.) Security and Cryptography for Networks, 6th International Conference, SCN 2008, Amalfi, Italy, September 10-12, 2008. Proceedings. Lecture Notes in Computer Science, vol. 5229, pp. 375–391. Springer (2008). https://doi.org/10.1007/978-3-540-85855-3_25
19. Jarecki, S., Liu, X.: Efficient oblivious pseudorandom function with applications to adaptive ot and secure computation of set intersection. In: Reingold, O. (ed.) Theory of Cryptography. LNSC, vol. 5444, pp. 577–594. Springer Berlin Heidelberg, Berlin, Heidelberg (2009)
20. Lewko, A., Waters, B.: New techniques for dual system encryption and fully secure hibe with short ciphertexts. In: Proceedings of the 7th International Conference on Theory of Cryptography. p. 455–479. TCC'10, Springer-Verlag, Berlin, Heidelberg (2010). https://doi.org/10.1007/978-3-642-11799-2_27
21. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakley, G.R., Chaum, D. (eds.) Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings. Lecture Notes in Computer Science, vol. 196, pp. 47–53. Springer (1984). https://doi.org/10.1007/3-540-39568-7_5
22. Waters, B.: Efficient identity-based encryption without random oracles. In: Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques. p. 114–127. EUROCRYPT'05, Springer-Verlag, Berlin, Heidelberg (2005). https://doi.org/10.1007/11426639_7, https://doi.org/10.1007/11426639_7
23. Wee, H.: Déjà Q: encore! un petit IBE. In: Kushilevitz, E., Malkin, T. (eds.) Theory of Cryptography - 13th International Conference, TCC 2016-A, Tel Aviv, Israel, January 10-13, 2016, Proceedings, Part II. Lecture Notes in Computer Science, vol. 9563, pp. 237–258. Springer (2016). https://doi.org/10.1007/978-3-662-49099-0_9

A Efficient Instantiation of HE

We instantiate the encryption scheme with additively homomorphic encryption of [19], which was a variant of Camenisch-Shoup encryption [5].

- $\mathsf{Primes}(1^{\lambda})$ outputs p_1, p_2 s.t. $p_1 = 2p_1' + 1$, $p_2 = 2p_2' + 1$, and p_1, p_2, p_1' and p_2' are all primes of length $\Theta(\lambda)$.
- $\mathsf{Setup}(p_1, p_2)$ outputs $par = (g, n)$ where n is safe RSA modulo, *i.e.* $n = p_1 \cdot p_2$, and g is of order $p_1' \cdot p_2'$. Let $h = n + 1$ and $n' = p_1' \cdot p_2'$. The message space $\mathcal{M}$ is the additive group $\mathbb{Z}_n$.
- $\mathsf{KeyGen}(par)$ picks a random value x in $[0, \frac{n}{4}]$, computes $y = g^x$, and sets $(pk, sk) = (y, x)$.
- $\mathsf{Enc}(pk, m)$ for $m \in \mathcal{M}$, picks a random value $r \in [0, \frac{n}{4}]$, and outputs a ciphertext $C = (u, e) = (g^r, y^r h^m)$.
- $\mathsf{Dec}(sk, (u, e))$ computes $\hat{m} = (e/ux)^2$. If $\hat{m} \in \langle h \rangle$ (i.e. if n does not divide $\hat{m} - 1$), it rejects the ciphertext. Otherwise, it sets $\hat{m}' = \frac{\hat{m}-1}{n}$ (over integers), computes $\gamma = \beta^{-1} \mod n$, and outputs $m = \hat{m}'/2 \cdot \gamma \mod n$.

B Other vulnerable IBE schemes

Lewko and Waters IBE [20]. Another IBE construction in the standard model is Lewko and Waters IBE [20]. Here, $params$, msk and ct_{id} are defined as follows:

$$params = (u, g, h, e(g, g)^{\alpha}), msk = (\alpha, g_3), ct_{id} = (m \cdot e(g, g)^{\alpha s}, (u^{id} h)^s, g^s)$$

Here, the KGC can compute $e(g, g^s)^{\alpha}$ using the msk and compute the message m from the ciphertext by removing the mask $e(g, g)^{\alpha s}$.

C Proofs of Lemmas

Proof of lemma 1. Assume the existence of a distinguisher $\mathcal{A}$, we can build an adversary $\mathcal{A}_1'$ using $\mathcal{A}$ which can break the decision subgroup assumption with non-negligible probability. The description of $\mathcal{A}_1'$ is as follows:

1. On input $(par_1, par_2, \mathsf{H}, Z)$ from the challenger $\mathcal{C}$, $\mathcal{A}_1'$ runs rest of the $\mathsf{Setup}(\lambda)$ and send $(params, mpk)$ to $\mathcal{A}$.
2. On receiving key-extraction queries on identities $id_1, \ldots, id_q$ from $\mathcal{A}$, $\mathcal{A}_1'$ aborts if the proof does not verify. Otherwise, it extracts id_i from π_i, computes and sends (C_{sk_i}, val_i) to $\mathcal{A}$.
3. On input (m^*, id^*) from $\mathcal{A}$ as the challenge query, $\mathcal{A}_1'$ compute sk_{id^*}, $C_0 = (Z, \mathsf{H}(e(Z, sk_{id^*})) \oplus m^*)$, $C_1 \leftarrow \mathsf{CTSamp}(params, mpk)$ and sends C_b to $\mathcal{A}$ where b is the random bit.
4. When $\mathcal{A}$ sends its guess as $\mathsf{Game}\ 3$, $\mathcal{A}_1'$ forwards $b' = 0$ to $\mathcal{C}$. Else, $\mathcal{A}_1'$ forwards $b' = 1$ to the challenger.

When the challenger samples $Z \leftarrow G_{p_1}$, the view of the adversary $\mathcal{A}$ is equivalent to $\mathsf{Game\ 3}$. When the challenger samples $Z \leftarrow G_{p_1}G_{p_2}$, the view of the adversary corresponds to $\mathsf{Game\ 4}$. The reduction simulates both games perfectly. Thus, $Adv_3 - Adv_4 \leq Adv^{SD_1,G}_{\mathcal{A}'_1}$ holds. □

Proof of lemma 2. An adversary $\mathcal{A}$ that can distinguish between the games can be used to build an adversary $\mathcal{A}'_2$ which breaks the semantic security of the encryption scheme HE.

The description of $\mathcal{A}'_2$ is as follows:

1. On receiving the public key pk and public parameters $(par_1, par_2, \mathsf{H})$ from the challenger $\mathcal{C}$, it sets $pk_{\mathcal{KGC}} = pk$ and generates other values in $params$ and mpk.
2. To generate C_α in mpk, it sends α, α' to $\mathcal{C}$.
3. Upon receiving ct from $\mathcal{C}$, it sends $(params, mpk)$ to $\mathcal{A}$ where $C_\alpha = ct$.
4. On receiving key queries from $\mathcal{A}$, it extracts id_i from π_i and sends (C_{sk_i}, val_i) to $\mathcal{A}$.
5. On receiving challenge query from $\mathcal{A}$, compute $C_0 = (C, \mathsf{H}(e(C, sk_{id^*})) \oplus m^*)$ and $C_1 \leftarrow \mathsf{CTSamp}(params,$
$mpk)$. Send C_b depending on a challenge bit $b \leftarrow \{0,1\}$.
6. When $\mathcal{A}$ sends its guess as $\mathsf{Game\ 4}$, $\mathcal{A}'_1$ forwards $b' = 0$ to $\mathcal{C}$. Else, $\mathcal{A}'_1$ forwards $b' = 1$ to $\mathcal{C}$.

□

Proof of lemma 3. We proceed via a sequence of sub-games Sub-Game 6.j.0 and Sub-Game 6.j.1 for j=1,2,. . . , q+2. Let Sub-Game 6.0.1 be Game 5 and the Sub-Game 6.q+2.1 corresponds to Game 6.
In Sub-Game 6.j.0, the following changes to Game 5 are made. Sample $r_1, \ldots, r_j \leftarrow \mathbb{Z}_N$.

$$mpk := (g_1, g_1^\alpha, e(g_1, uh_2^{vr_1+\cdots+vr_j}), hh_2^{r_1+\cdots+r_j}, pk_{\mathsf{KGC}}, C_\alpha)$$

For all $i \in [j], val_i := h^{\frac{v}{\alpha+id_i}-\sigma_{v_i}} h_2^{r_j\left(\frac{v}{\alpha+id_i}-\sigma_{v_i}\right)+r_{j-1}\left(\frac{v}{\alpha_{j-1}+id_i}-\sigma_{v_i}\right)+\cdots+r_1\left(\frac{v}{\alpha_1+id_i}-\sigma_{v_i}\right)}$

$$sk_{id^*} := h^{\frac{v}{\alpha+id^*}} h_2^{\frac{vr_j}{\alpha+id^*}+\frac{vr_{j-1}}{\alpha_{j-1}+id^*}+\cdots+\frac{vr_1}{\alpha_1+id^*}}$$

In Sub-Game 6.j.1, we make the following changes to Game 5 . Sample $r_1, \ldots, r_j \leftarrow \mathbb{Z}_N$.

$$mpk = (g_1, g_1^\alpha, e(g_1, uh_2^{vr_1+\cdots+vr_j}), hh_2^{r_1+\cdots+r_j}, pk_{\mathsf{KGC}}, C_\alpha)$$

$$\text{For all } i \in [j], val_i = h^{\frac{v}{\alpha+id_i}-\sigma_{v_i}} h_2^{r_j\left(\frac{v}{\alpha_j+id_i}-\sigma_{v_i}\right)+\cdots+r_1\left(\frac{v}{\alpha_1+id_i}-\sigma_{v_i}\right)}$$

$$sk_{id^*} = h^{\frac{v}{\alpha+id^*}} h_2^{\frac{vr_j}{\alpha_j+id^*}+\cdots+\frac{vr_1}{\alpha_1+id^*}}$$

Lemma 13. *$Adv_{6.j.0} = Adv_{6.j.1}$ for $j = 1, 2, \ldots, q+2$.*

As α mod p_2 is hidden given mpk, we can replace α mod p_2 with α_j mod p_2 in the exponent of h_2 in both val_i and sk_{id^*}.

Lemma 14. *$Adv_{6.j-1.1} - Adv_{6.j.0} \leq Adv_{\mathcal{A}'_3}^{SD_2,H}$ for $j = 1, 2, \ldots, q+2$, where $Adv_{\mathcal{A}'_3}^{SD_2,H}$ is the advantage of an adversary in the sub-group decision assumption game SD_2 in H.*

Proof of lemma 14. Assume the existence of a distinguisher $\mathcal{A}$ which can distinguish between the sub-games. We build an adversary $\mathcal{A}'_3$ that can break the decision subgroup assumption SD_2 with non-negligible probability. The description of $\mathcal{A}'_3$ is as follows:

1. On input $(par_1, par_2, \mathsf{H}, h_2, Z)$ from the challenger $\mathcal{C}$, sample $\alpha_1 \ldots \alpha_{j-1}, r_1, \ldots, r_{j-1} \leftarrow \mathbb{Z}_N$. Compute $mpk := (g_1, g_1^{\alpha}, e(g_1, Z^v h_2^{vr_1+\cdots+vr_{j-1}}), Z{\cdot}h_2^{r_1+\cdots+r_{j-1}}, pk_{\mathsf{KGC}}, C_\alpha)$, and send $(params, mpk)$ to $\mathcal{A}$.
2. On key-extraction queries from $\mathcal{A}$, extract id_i, and send $(C_{sk_i},\, val_i = Z^{\frac{v}{\alpha+id_i}-\sigma_{v_i}} h_2^{r_{j-1}(\frac{v}{\alpha_{j-1}+id_i}-\sigma_{v_i})+\cdots+r_1(\frac{v}{\alpha_1+id_i}-\sigma_{v_i})})$ to $\mathcal{A}$.
3. On input (m^*, id^*) from $\mathcal{A}$, $\mathcal{A}'_3$ computes $sk_{id^*} = Z^{\frac{v}{\alpha+id^*}} h_2^{(\frac{vr_{j-1}}{\alpha_{j-1}+id^*}+\cdots+\frac{vr_1}{\alpha_1+id^*})}$. Compute $C_0 := (C, \mathsf{H}(e(C, sk_{id^*})) \oplus m^*)$ where $C \leftarrow G$, $C_1 \leftarrow \mathsf{CTSamp}(params, mpk)$ and send C_b to $\mathcal{A}$ where b is a random bit.
4. When $\mathcal{A}$ sends its guess as Sub-Game 6.j-1.1, $\mathcal{A}'_3$ forwards $b' = 0$ to $\mathcal{C}$. Otherwise, $\mathcal{A}'_3$ forwards $b' = 1$ to the challenger.

When the adversary $\mathcal{A}$ outputs the result as Sub-Game 6.j-1.1, $\mathcal{A}'_3$ forwards $b' = 0$ and $\mathcal{A}'_3$ forwards $b' = 1$ otherwise. Both the sub-games are perfectly simulated. Thus, the advantage $Adv_{6.j-1.1} - Adv_{6.j.0} \leq Adv_{\mathcal{A}'_3}^{SD_2,H}$. □

Combining all the previous arguments,

$$Adv_5 - Adv_6 \leq (q+2) \cdot Adv_{\mathcal{A}'_3}^{SD_2,H}$$

□

Proof of lemma 5. The proof of this lemma uses arguments similar to Lemma 3 in [14]. We need to show that

$$\left(\prod_{i=1}^{q+2}\prod_{j=1}^{q+1}(\alpha_i + id_j)\right) \cdot \det(B) = \delta \cdot \left(\prod_{1 \leq i < j \leq q+1} (id_i - id_j)\right)\left(\prod_{1 \leq i < j \leq q+2} (\alpha_i - \alpha_j)\right) \cdot$$

We can represent $\det(B)$ as the sum of inverses of homogeneous polynomials of degree $q+1$. Multiplying it with $\prod_{i=1}^{q+2}\prod_{j=1}^{q+1}(\alpha_i + id_j)$ will remove the denominators and results in a homogeneous polynomial P in $\alpha_1, \ldots, \alpha_{q+2}, id_1, \ldots, id_{q+1}$ of degree,

$$(q+1)(q+2) - (q+1) = (q+1)^2 \cdot$$

Also, note that $\det(B) = 0$ if

- $\alpha_i = \alpha_j$ where $i \neq j$ and $i, j \in [q+2]$,
- $id_i = id_j \mod p_2$ where $i \neq j$ and $i, j \in [q+1]$.

Thus, P must be a multiple of $Q = \prod_{1 \leq i < j \leq q+1} (id_i - id_j) \prod_{1 \leq i < j \leq q+2} (\alpha_i - \alpha_j)$. The degree of polynomial Q is,

$$\frac{q(q+1)}{2} + \frac{(q+2)(q+1)}{2} = (q+1)^2 \cdot$$

which is equal to the degree of polynomial P. Therefore, P must be a constant multiple of Q. □

Proof of lemma 7. If there exists $\mathcal{A}$ that can differentiate between Game 0 and Game 1, then, we can build $\mathcal{A}'$ that uses $\mathcal{A}$ to distinguish real proofs from simulated proofs. The advantage of $\mathcal{A}'$ in distinguishing real/simulated proofs is $Adv_0 - Adv_1 \leq q \cdot Adv_{\mathcal{A}'}$, which is negligible by the zero-knowledge property of the proof system. □

Proof of lemma 8. We proceed through a series of sub-games. The Sub-Game 2.0 is Game 1 and Sub-Game 2.q be Game 2. In Sub-Game 2.j, $C_i = \mathsf{HE.Enc}(pk_{u_i}, a'_i)$ for $i \leq j$ and $C_i = \mathsf{HE.Enc}(pk_{u_i}, a_i)$ otherwise. If there exists an adversary $\mathcal{A}$ that can distinguish between the sub-games, then $\mathcal{A}'_1$ can use $\mathcal{A}$ to break the security of the underlying homomorphic encryption scheme. $\mathcal{A}'_1$ is described as follows.

1. On receiving $(par_1, par_2, \mathsf{H}, pk_u)$, computes $(params, mpk, msk)$ and forwards to $\mathcal{A}$.
2. For all $i \in [q], i \neq j$, $(pk_{u_i}, sk_{u_i}) \leftarrow \mathsf{HE.KeyGen}(g, N) \cdot$
3. When $\mathcal{A}$ submits i^{th} BlindExtract query, where $i \in [q]$,
   (a) For $i < j$, sample $id_i \leftarrow \mathcal{I}$ and update $\mathsf{IDList}[i] := id_i$. Sample $a_i, a'_i \in \mathbb{Z}_N$, send $(pk_{u_i}, C_{a_i} := \mathsf{HE.Enc}(pk_{u_i}, a'_i), C_{id_i} := (C_\alpha \cdot \mathsf{HE.Enc}(pk_{\mathcal{KGC}}, id_i)^{a_i}, \pi_i)$ to $\mathcal{A}$.
   (b) For $i = j$, $\mathcal{A}'_1$ samples $a, a' \leftarrow \mathbb{Z}_N$ and sends it to the challenger $\mathcal{C}$. On receiving C from $\mathcal{C}$, sample $id_j \leftarrow \mathcal{I}$, update $\mathsf{IDList}[j] := id_j$, and send $(pk_u, C, C_{id_j} := (C_\alpha \cdot \mathsf{HE.Enc}(pk_{\mathcal{KGC}}, id_j)^a, \pi_j)$ to $\mathcal{A}$.
   (c) For $i > j$, sample $id_i \leftarrow \mathcal{I}$ and sets $\mathsf{IDList}[i] := id_i$. Also, sample $a_i \leftarrow \mathbb{Z}_N$, sends $(pk_{u_i}, C_{a_i} := \mathsf{HE.Enc}(pk_{u_i}, a_i), C_{id_i} := (C_\alpha \cdot \mathsf{HE.Enc}(pk_{\mathcal{KGC}}, id_i)^{a_i}, \pi_i)$ to $\mathcal{A}$.
4. On receiving the index i^* and message m^* from $\mathcal{A}$, and if i^*-th BlindExtract query was already queried, set $id^* := \mathsf{IDList}[i^*]$, and compute $C_0 = (g_1^{(\alpha+id^*)s}, \mathsf{H}(e(g_1, u)^s) \oplus m^*)$ and $C_1 \leftarrow \mathsf{CTSamp}(params, mpk)$. Sample $b \leftarrow \{0, 1\}$ and send C_b.
5. Forwards the guess from $\mathcal{A}$ to $\mathcal{C}$.

When the challenger picks $b = 0$ and sends $C = \mathsf{HE.Enc}(pk_u, a)$, the view of $\mathcal{A}$ is the same as $\mathsf{Sub\text{-}Game\ 2.j\text{-}1}$. Similarly, if the challenger picks $b = 1$ and computes $C = \mathsf{HE.Enc}(pk_u, a')$, then the view of the adversary is the same as $\mathsf{Sub\text{-}Game\ 2.j}$. So, the reduction perfectly simulates the games. Thus, $Adv_{2.j-1} - Adv_{2.j} \leq Adv^{\mathsf{HE}}_{\mathcal{A}'_1}$ and therefore $Adv_{2.0} - Adv_{2.q} \leq q \cdot Adv^{\mathsf{HE}}_{\mathcal{A}'_1}$. □

Proof of lemma 9. We can build an adversary $\mathcal{A}'_2$ using a distinguisher $\mathcal{A}$ to break the sub-group decision assumption. The description of $\mathcal{A}'_2$ is as follows:

1. On receiving $(par_1, par_2, \mathsf{H}, Z)$ from the challenger $\mathcal{C}$, computes $(params, mpk, msk)$ and sends it to $\mathcal{A}$.
2. When $\mathcal{A}$ submits i^{th} $\mathsf{BlindExtract}$ query where $i \in [q]$, sample $id_i \leftarrow \mathcal{I}$, sets $\mathsf{IDList}[i] := id_i$. Sample $a'_i, r'_i \leftarrow \mathbb{Z}_N$, generates $(pk_{u_i}, sk_{u_i}) \leftarrow \mathsf{HE.KeyGen}(g, N)$, compute and send $(pk_{u_i}, C_{a_i}, C_{id_i}, \pi_i)$ to $\mathcal{A}$.
3. On receiving m^* and i^* from $\mathcal{A}$, and if i^*-th $\mathsf{BlindExtract}$ query was already queried, set $id^* := \mathsf{IDList}[i^*]$, compute $C_0 = (Z, \mathsf{H}(e(Z, sk_{id^*})) \oplus m^*)$ and $C_1 \leftarrow \mathsf{CTSamp}(params, mpk)$. Send C_b to $\mathcal{A}$.
4. If $\mathcal{A}$ sends its guess as $\mathsf{Game\ 4}$, $\mathcal{A}'_2$ sends $b' = 0$ to $\mathcal{C}$. Otherwise, $\mathcal{A}'_2$ sends $b' = 1$ to $\mathcal{C}$.

The adversary $\mathcal{A}'_2$ simulates the two games perfectly. Thus, the view of $\mathcal{A}$ is $\mathsf{Game\ 4}$ or $\mathsf{Game\ 5}$ depending on challenge bit b. From thr sub-group decision assumption, $Adv_4 - Adv_5 \leq Adv^{SD_1,G}_{\mathcal{A}'_2}$ holds. □

Proof of lemma 10. Let $\mathsf{Sub\text{-}Game\ 5.1}$ be the sub-game with the following values where $r_1 \leftarrow \mathbb{Z}_N$:

$$mpk := (g_1, g_1^{\alpha}, e(g_1, h^v h_2^{vr_1}), hh_2^{r_1}, pk_{\mathcal{KGC}}, C_{\alpha})$$

$$msk := (\alpha, v, h^v h_2^{vr_1}, sk_{\mathcal{KGC}})$$

$$sk_{id^*} := h^{\frac{v}{\alpha+id^*}} h_2^{r_1 \frac{v}{\alpha+id^*}}$$

Lemma 15. *Assuming the decision subgroup assumption SD_2 in H , $Adv_5 - Adv_{5.1} \leq Adv^{SD_2,H}_{\mathcal{A}'_3}$.*

Proof of lemma 15. We prove the above lemma through a reduction to the subgroup decision assumption game. Assume there exists an adversary $\mathcal{A}$ that can distinguish the $\mathsf{Game\ 5}$ and $\mathsf{Sub\text{-}Game\ 5.1}$, we can build $\mathcal{A}'_3$ that uses $\mathcal{A}$ to break the decision subgroup assumption SD_2. The description of $\mathcal{A}'_3$ is as follows:

1. On receiving $(par_1, par_2, \mathsf{H}, h_2, Z)$ from the challenger $\mathcal{C}$, runs the rest of the Setup by sampling $v \leftarrow \mathbb{Z}_N$. Compute $mpk = (g_1, g_1^{\alpha}, e(g_1, Z^v), Z, pk_{\mathcal{KGC}}, C_{\alpha})$, $msk = (\alpha, v, Z^v, sk_{\mathcal{KGC}})$ and send both to the adversary $\mathcal{A}$.
2. When $\mathcal{A}$ submits i^{th} $\mathsf{BlindExtract}$ query, where $i \in [q]$, pick $id_i \leftarrow \mathbb{Z}_N$, and set $\mathsf{IDList}[i] := id_i$. Also, generates $(pk_{u_i}, sk_{u_i}) \leftarrow \mathsf{HE.Enc}(g, N)$, compute and send $(pk_{u_i}, C_{a_i}, C_{id_i}, \pi_i)$ to $\mathcal{A}$ where $a'_i, r'_i \leftarrow \mathbb{Z}_N$.

3. On receiving i^* and m^* from $\mathcal{A}$, and if i^*-th $\mathsf{BlindExtract}$ query was already queried, set $id^* = \mathsf{IDList}[i^*]$. Computes $C_0 = (C, H(e(C, Z^{\frac{v}{\alpha+id^*}})) \oplus m^*)$ and $C_1 \leftarrow \mathsf{CTSamp}(params, mpk)$. Sends C_b to $\mathcal{A}$ where $b \leftarrow \{0,1\}$.
4. Forwards the guess from $\mathcal{A}$ to $\mathcal{C}$.

On input challenge, either $Z = h \leftarrow H_{p_1}$ or $Z = hh_2^{r_1} \leftarrow H_{p_1}H_{p_2}$. When $Z = h \leftarrow H_{p_1}$, the resulting game is $\mathsf{Game\ 5}$ and when $Z = hh_2^{r_1} \leftarrow H_{p_1}H_{p_2}$, the view of $\mathcal{A}$ is the same as $\mathsf{Sub\text{-}Game\ 5.1}$ as any element in H_{p_2} can be represented by $h_2^{r_1}$. The view of $\mathcal{A}$ is simulated correctly, $Adv_5 - Adv_{5.1} \leq Adv_{\mathcal{A}'_3}^{SD_2,H}$. □

We describe $\mathsf{Sub\text{-}Game\ 5.2}$ below by modifying the following values, sample $id_a \leftarrow \mathcal{I}$.

$$sk_{id^*} := h^{\frac{v}{\alpha+id^*}} h_2^{r_1 \frac{v}{\alpha+id_a}}.$$

Lemma 16. $Adv_{5.1} \approx Adv_{5.2}$.

The value $id^* \mod p_2$ is hidden from the adversary given $(params, mpk, msk)$. Thus, we can replace id^* in the exponent of h_2 with a random element in the identity space.

Remark 1. To solve the key-escrow problem, we will need to place some restrictions on the identity space. Otherwise, if the identity distribution is highly skewed, the KGC can guess the identity of the user with a high probability. In this work, we consider that the identities of the users are uniformly distributed. Another solution would be to allow the identity space to have a large enough min-entropy. Our proof should be modified to accommodate these changes, and we leave this as future work.

$\mathsf{Sub\text{-}Game\ 5.3}$ We modify the values, sample $r_1, r_2 \leftarrow \mathbb{Z}_N$, $id_a \leftarrow \mathcal{I}$.

$$mpk := (g_1, g_1^{\alpha}, , e(g_1, h^v h_2^{v(r_1+r_2)}), hh_2^{r_1+r_2}, pk_{\mathcal{KGC}}, C_{\alpha})\cdot$$

$$msk := (\alpha, v, h^v h_2^{v(r_1+r_2)}, sk_{\mathcal{KGC}})\cdot$$

$$sk_{id^*} := h^{\frac{v}{\alpha+id^*}} h_2^{r_1 \frac{v}{\alpha+id_a} + r_2 \frac{v}{\alpha+id^*}}.$$

Lemma 17. $Adv_{5.2} - Adv_{5.3} \leq Adv_{\mathcal{A}'_3}^{SD_2,H}$.

We omit the proof of the above lemma as it is similar to the proof of the previous lemma 15, $Adv_5 - Adv_{5.1} \leq Adv_{\mathcal{A}'_3}^{SD_2,H}$.

Lemma 18. $Adv_{5.3} \approx Adv_6$.

In $\mathsf{Game\ 6}$, id^* in the exponent of h_2 is replaced with a random value id_b. Since $id^* \mod p_2$ is hidden from $(params, mpk, msk)$, this modification does not change the adversary's advantage. □