Semantic Definition of Anonymity in Identity-Based Encryption and Its Relation to Indistinguishability-Based Definition

Goichiro Hanaoka[1], Misaki Komatsu[2], Kazuma Ohara[1], Yusuke Sakai[1], and Shota Yamada[1(✉)]

[1] National Institute of Advanced Industrial Science and Technology (AIST), 2-4-7 Aomi, Koto-ku, Tokyo 135-0064, Japan
{hanaoka-goichiro,ohara.kazuma,yusuke.sakai,yamada-shota}@aist.go.jp
[2] Toshiba Corporation Corporate Research & Development Center, 1 Komukai-Toshiba-cho, Saiwai-ku Kawasaki-shi, Kanagawa 212-8582, Japan
misaki1.komatsu@toshiba.co.jp

Abstract. In this paper we point out an overlooked subtlety in providing proper security definitions of anonymous identity-based encryption (anonymous IBE) and its applications such as searchable encryption. Namely, we find that until now there is no discussion whether the widely used indistinguishability-based notion of anonymity for IBE implies simulation-based definition of anonymity, which directly captures the intuition that recipients' IDs are not leaked from ciphertexts. We compensate this undesirable situation by providing a simulation-based notion, which requires that a ciphertext can be simulated without knowing the associated ID, by specializing the anonymity notion defined for more generalized notion of attribute-based encryption in previous work to the setting of IBE and then proving that this definition is equivalent to the conventional indistinguishability-based definition. We note that while the final result is something one would expect, our proof is not completely trivial. In particular, previous proofs that show the equivalence between semantic security and indistinguishability-based one in the setting where the security of payload is the main concern do not work immediately in our setting due to the difference between the semantics of identities and messages and the existence of the key extraction oracles.

Keywords: Identity-based encryption · Anonymity · Semantic security

1 Introduction

We identify an overlooked issue in the security definitions of the anonymous identity-based encryption (anonymous IBE) and application thereof such as searchable encryption. In particular, we point out that there are no arguments

L. Chen et al. (Eds.): ESORICS 2020, LNCS 12309, pp. 65–85, 2020.
https://doi.org/10.1007/978-3-030-59013-0_4

on the relation between commonly accepted indistinguishability definition for anonymity and simulation-based one, where the latter directly captures the intuition that recipients' IDs are not leaked from ciphertexts. In this paper, we fill this gap and for the first time demonstrate that the widely accepted indistinguishability-based definition implies a simulation-based definition.

1.1 Background

Searchable Encryption. Searchable encryption is today one of the active research trends in cryptography. Searchable encryption allows to search a piece of information over an encrypted data, while keeping the data content and the query secret even from the server holding the encrypted data.

With the rapid development of information technology, such as cloud computing, the guarantee of user privacy (without compromising usability as much as possible) has become an important issue for service providers. Therefore, searchable encryption has attracted a lot of attention as a method to realize encrypted databases (EDB). Since CryptDB [37] demonstrated the practicality of its approach, a number of EDBs have been proposed [2,42]. The fact that there are many commercial EDB among them (such as Microsoft SQL Server [34], Google Encrypted Big Query [25], SAP SEEED [26]) shows the demand for EDBs. In recent days, startups [3,18,41] also developed products and services based on searchable encryption.

In academia, searchable encryption is still actively being studied from functional aspects such as range queries [29] and conjunctive queries [23,35], efficiency aspects such as trade-off between storage size and search efficiency [4,5,15,19,20], and security aspects such as verifiability [32,44].

Relation to Anonymous IBE. It is widely believed that these searchable encryption schemes are proven secure under some appropriate security definitions. In particular, (public-key) searchable encryption can be constructed from anonymous identity-based encryption (anonymous IBE), and thus such searchable encryption schemes is believed to be secure if the underlying anonymous IBE is secure. Furthermore, it is worth noting that an anonymous IBE scheme can be constructed from a public-key searchable encryption scheme [9], these two cryptographic primitives are in fact equivalent.

Overlooked Issue in the Security Definitions. However, there seems to be an overlooked subtlety in the theoretical efforts to construct secure searchable encryption schemes. Concretely, a number of public key encryption with key word search (PEKS) schemes are mostly based on indistinguishability (IND)-based security [1,9,12] and there has been no discussion on the notion for semantic security (SS), whereas the security for symmetric searchable encryption (SSE), which is a symmetric-key variant of PEKS, are proven SS-based definition. In many cases, SS-based and IND-based definitions achieve same level of security, however, it is also known that IND and SS are not equivalent in some cases [11].

Therefore, there is a room for consideration on the difference between the security on PEKS and SSE, and discussion for the SS-based security on PEKS would help to properly understand the security of these schemes. As mentioned above, one of the most basic construction of PEKS is based on anonymous IBE, and the confidentiality of keywords in PEKS corresponds to the anonymity of the identity in the IBE. The anonymity of IBE has also been proposed so far with only the IND-based definition, and the SS-based is not known. That is, it would be worth considering about SS-based definition for anonymity in IBE, as a first step for considering SS-based security in PEKS.

Remind that Goldwasser and Micali introduced the IND-CPA definition (indistinguishability against chosen-plaintext attacks) [24] as an easy-to-deal-with alternative of semantic security [24]. Semantic security is meant to directly capture our intuition that the adversary learns nothing on the plaintext from a ciphertext, which is expressed in terms of a simulation-based definition. However, this definition is complex and not easy to deal with. Contrary to this, IND-CPA is less intuitive and does not directly capture the idea of not leaking any partial information of the encrypted message, but is simple and easy to deal with. Goldwasser and Micali proved that these definitions are equivalent. Therefore, by only proving a public-key encryption scheme is secure under the IND-CPA definition we can confirm that the scheme satisfies more intuitive notion of semantic security.

Their approach is generalized to formalize the security of various cryptographic primitives. In general, we consider that the simulation-based security notion as a preferable goal for cryptographic primitives to achieve compared to IND-based notion. This is because the former seems to be more intuitive and is usually at least as strong as the latter. If we can prove that both security notions are in fact equivalent, we can use IND-based definition as a handy alternative for the simulation-based security. However, it is possible for (appropriately defined) IND-based and simulation-based definitions not to be equivalent, which is evidenced by some separation results between IND-based and simulation-based definitions in various cryptographic primitives and notions, such as functional encryption [11], security against selective-opening attacks [8], and non-malleability [36].

1.2 Our Contribution

In this paper, we provide a simulation-based definition of anonymity for IBE and study the relationship between this simulation-based definition and the conventional IND-based definition of anonymity. In more details, we define the simulation-based definition of anonymity of IBE by specializing Wee's definition of anonymity for attribute-based encryption [28] to the setting of IBE. Then, we investigate the two directions of implications, namely, *(i) whether the simulation-based definition implies the IND-based definition*, and *(ii) whether the IND-based definition implies the simulation-based definition*. These establish the equivalence between the two notions.

While the result is something one would expect, we emphasize that our proof for the latter direction (ii) is not straightforward. In particular, previous proofs [6,24] that show the equivalence between semantic security and IND-based one in the setting where the security of payload is the main concern do not work immediately in our setting due to the difference between the semantics of identities and messages and the existence of the key extraction oracles. In more details, in our setting, we have to come up with a reduction that abides by the restriction on key extraction queries, which is not present in the payload hiding settings. The crux of the proof boils down to showing that the adversary is unable to make a key query for certain identity with more than negligible probability. In order to prove this, we introduce several game hops and crucially use the IND-based security of the IBE. We refer to Sect. 4 for details.

This result for the first time shows that the IND-based anonymity definition implies the simulation-based anonymity definition. This implies that the existing IBE schemes secure under the IND-based anonymity definition indeed do not leak recipients' IDs. In addition, this fact not only guarantees the security of the IBE schemes proven secure under the IND-based definition, does it allow us to keep using the easy-to-use IND-based definition as we did.

However, the fact that our proof is not trivial suggests that the equivalence between indistinguishability-based definition and simulation-based one is not necessarily always true. Indeed, the difference between the two security notions has been identified for the case of functional encryption and selective opening security (Please refer to the next subsection for more discussion). Our conclusion is that it would be risky to prove the secrecy of information in an IND-based style for some primitive and use it as if it also satisfied simulation-based security without a careful consideration.

1.3 Related Work

The idea of IBE is due to Shamir [39], and first practical solutions were proposed by Sakai et al. [38], Boneh et al. [10], Cocks [17] independently. In particular, Boneh et al. have provided a definition of plaintext secrecy in the IBE, which has been standardly used until today. The definition by Boneh et al. was based on IND, and thus SS-based security was not strictly discussed at first, but Attrapadung et al. [6] later showed the equivalence of both definitions. Later, Izabachene et al. [30] discussed various definitions of plaintext secrecy and their relations. Abdalla et al. [1] defined the anonymity of IBE based on IND (namely, Ano-LOR), and many follow-up works adopted the IND-based definition of anonymity or variants thereof [7,13,14,22,27,31,33,43]. However, since the introduction of the IND-based definition of anonymity, there has been little in-depth study on the definition on anonymity, and in particular, the concrete formulation of the definition based on SS and its relation to the IND-based definition were not well understood. Notably Boneh et al. [11] indicates that security definitions based on IND and SS may not be equivalent in functional encryption, which is a superordinate concept of IBE.

2 Preliminaries

In this section, we first denote notations used in this work. Then we give syntax and correctness of Identity-Based Key Encapsulation Mechanism (IB-KEM). After that, we present two security notions for IB-KEM, namely, IND-ID-CPA and Ano-LOR.

Notations. For set Y, $y \leftarrow Y$ denotes that y is uniformly chosen from Y. If Y is a function or algorithm, it denotes that Y outputs y. By PPT, we denote a probabilistic polynomial-time algorithm. For PPT algorithm A, $A^{\mathcal{O}}$ denotes that A has access to the oracle $\mathcal{O}$. $\perp$ is a symbol that means failure of decryption. Throughout, we use 1^k as the security parameter. A function $\varepsilon(k)$ is negligible if for any $c > 0$ there exists an $k_c > 0$ such that, for all $k > k_c$ we have: $\varepsilon(k) < k^{-c}$.

2.1 Identity-Based Key Encapsulation Mechanism

Here, we define Identity-Based Key Encapsulation Mechanism (IB-KEM). While the main focus of this paper is on the security definition of anonymous IBE, using IB-KEM instead will simplify the discussion. We can convert IB-KEM to IBE by using appropriate secret key encryption.

Syntax. An IB-KEM scheme Σ is a tuple (S, K, E, D) of PPT algorithms, where $\mathcal{ID}$ is a identity space and $\mathcal{K}$ is a symmetric-key space.

$S(1^k)$: The setup algorithm gets as input the security parameter 1^k. It outputs the public parameter prm, and the master secret key msk. We assume prm is implicitly provided as input to all algorithms.
$K(msk, id)$: The key generation algorithm gets as input the msk, and $id \in \mathcal{ID}$. It outputs a user secret key usk_{id}.
$E(prm, id)$: The encryption algorithm gets as input prm, and $id \in \mathcal{ID}$. It outputs a ciphertext ct and a symmetric-key $kem \in \mathcal{K}$.
$D(ct, usk_{id})$: The decryption algorithm gets as input ct, and usk_{id}. It outputs kem or $\perp$.

Correctness. IB-KEM is said to have correctness if we consider probabilities for $(prm, msk) \leftarrow S(1^k)$, $usk_{id} \leftarrow K(msk, id)$ and $(ct, kem) \leftarrow E(prm, id)$, then $\Pr[kem = D(ct, usk_{id})] = 1$ holds.

2.2 Security Definitions for IB-KEM

We denote two security definitions for IB-KEM, namely, IND-ID-CPA and Ano-LOR.

Here, we define IND-ID-CPA security and Ano-LOR for IB-KEM. IND-ID-CPA security is an indistinguishability based security notion that stipulates that an encrypted message is hidden. On the other hand, SS-ID-CPA is more natural security notion that captures the intuition that any information of the message

is not leaked to the adversary. It is known that these two notions are equivalent [6]. The definition of IND-ID-CPA security in this paper is based on [6], where we adapted their definition to the IB-KEM setting. The definition of Ano-LOR is indistinguishability-based definition that is widely used in the literature.

IND-ID-CPA. Let $\Sigma = (S, K, E, D)$ be an IB-KEM scheme and $A = (A_1, A_2)$ be a PPT adversary. We consider the following experiments IND-ID-CPA-b for $b \in \{0, 1\}$.

$$\begin{aligned}
&\underline{\mathbf{Exp}^{\text{IND-ID-CPA-}b}_{\Sigma,A}(k)} \\
&(prm, msk) \leftarrow S(1^k); \\
&(id^*, s) \leftarrow A_1^{K(\,msk,\,\cdot\,)}(prm); \\
&(ct, kem) \leftarrow E(id^*, prm); \\
&kem_0 = kem;\ kem_1 \leftarrow \mathcal{K}; \\
&b' \leftarrow A_2^{K^{\{id^*\}}(msk,\cdot)}(ct, kem_b, s);
\end{aligned}$$

In the above, key generation oracle $K(\,msk, \cdot\,)$ gets as input the msk and arbitrary $id \in \mathcal{ID}$, and outputs a user secret key usk_{id} associated with id. A_1 cannot use the id^* that is queried to $K(\,msk, \cdot\,)$ as the target ID. If A_2 queries id^* to $K^{\{id^*\}}(msk, \cdot)$, $K^{\{id^*\}}(msk, \cdot)$ outputs $\perp$. We define the advantage $\mathbf{Adv}^{\text{IND-ID-CPA}}_{\Sigma,A}(k)$ as follows;

$$\begin{aligned}
&\mathbf{Adv}^{\text{IND-ID-CPA}}_{\Sigma,A}(k) \\
&\quad := |\Pr[\ \mathbf{Exp}^{\text{IND-ID-CPA-0}}_{\Sigma,A}(k) \to 1\ ] - \Pr[\ \mathbf{Exp}^{\text{IND-ID-CPA-1}}_{\Sigma,A}(k) \to 1\ ]|.
\end{aligned}$$

Definition 1 (IND-ID-CPA)**.** *We say that IB-KEM scheme $\Sigma = (S, K, E, D)$ is* IND-ID-CPA *secure if $\mathbf{Adv}^{\text{IND-ID-CPA}}_{\Sigma,A}(k)$ is negligible for any PPT adversary $A = (A_1, A_2)$.*

Ano-LOR. Let $\Sigma = (S, K, E, D)$ be an IB-KEM scheme and $B = (B_1, B_2)$ be a PPT adversary. We consider the following experiments Ano-LOR-b for $b \in \{0, 1\}$

$$\begin{aligned}
&\underline{\mathbf{Exp}^{\text{LOR-}b}_{\Sigma,B}(k)} \\
&(prm, msk) \leftarrow S(1^k); \\
&(id_0, id_1, s) \leftarrow B_1^{K(\,msk,\,\cdot\,)}(prm); \\
&(ct, kem) \leftarrow E(id_b, prm); \\
&b' \leftarrow B_2^{K^{\{id_0, id_1\}}(msk,\cdot)}(ct, kem, s);
\end{aligned}$$

In the above, key generation oracle $K(\,msk, \cdot\,)$ gets as input the msk, and arbitrary $id \in \mathcal{ID}$. It outputs a user secret key usk_{id} associated with id. B_1 cannot use the already queried ID to $K(\,msk, \cdot\,)$ as the target ID (id_0, id_1). If B_2

queries id_0 or id_1 to $K^{\{id_0,id_1\}}(msk,\cdot)$, $K^{\{id_0,id_1\}}(msk,\cdot)$ outputs $\perp$. We define the advantage $\mathbf{Adv}^{\mathrm{LOR}}_{\Sigma,B}(k)$ as follows;

$$\mathbf{Adv}^{\mathrm{LOR}}_{\Sigma,B}(k) := |\Pr[\mathbf{Exp}^{\text{LOR-0}}_{\Sigma,B}(k) \to 1] - \Pr[\mathbf{Exp}^{\text{LOR-1}}_{\Sigma,B}(k) \to 1].|.$$

Definition 2 (Ano-LOR)**.** *We say that IBE scheme $\Sigma = (S, K, E, D)$ is Ano-LOR secure if $\mathbf{Adv}^{\mathrm{LOR}}_{\Sigma,B}(k)$ is negligible for any PPT adversary $B = (B_1, B_2)$.*

Discussion of Ano-LOR. Ano-LOR already captures certain kind of security, but we do not know whether it captures more natural semantic security notion of anonymity because Ano-LOR is defined based on the notion of indistinguishability.

To make the point clearer, let us recall the relationship between the security notion of public key encryption (PKE), which is simpler than IBE. To capture the intuition that the adversary cannot learn any information about encrypted message, Goldwasser and Micali [24] introduced the notion of semantic security (SS). In addition, they also defined simpler, but less intuitive notion of indistinguishability (IND). As shown by them, these definitions are in fact equivalent. Thanks to their result, we can use the simpler IND security notion when we give a security proof for a PKE scheme.

3 Simulation-Based Definition of Anonymity

In this section, we provide our definition of anonymity for IB-KEM named Ano-SS. Our definition captures a natural notion of security that the adversary cannot get any information on ID associated with a ciphertext. To validate our definition, we prove that our security notion implies Ano-LOR.

3.1 Defining Ano-SS for IB-KEM

Here, we address semantic security style definition of the anonymity for IB-KEM that we call Ano-SS in the following. A natural starting point for doing so would be adapt the definition of semantic security by Goldwasser and Micali [24] to our setting. Since their security notion has been successfully extended to other primitives including IBE and the equivalence to indistinguishability security notions have been shown [6], this seems to be a promising approach. However, as we explain in Appendix A, it turned out that it is not straightforward to define the notion based on their approach. The difficulty stems from the fact that while most of the previous work defining semantic security including [6] focuses on the data privacy of IBE, we focus on the anonymity and asymmetry between message and identity prohibits us from naturally extending the security notion to our setting. We refer to Appendix A for more details. Alternatively, we provide our semantic security notion of anonymity for IB-KEM by specializing the definition by Wee [28] that is defined for more general notion of attribute-based encryption to the setting of IB-KEM.

Definition. In the following, we provide the special case of Wee's definition for anonymity [28] where we only consider IB-KEM instead of ABE. We call our definition Ano-SS. Let $\Sigma = (S, K, E, D)$ be an IB-KEM scheme and $C = (C_1, C_2)$ be a PPT adversary. We also let $\Sigma^* = (S^*, K^*, E^*)$ be a simulator, which possibly depends on the adversary. We consider the following two experiments $\mathbf{Exp}^{\text{SS-REAL}}_{\Sigma,C}(k)$ and $\mathbf{Exp}^{\text{SS-IDEAL}}_{\Sigma,\Sigma^*,C}(k)$.

$\underline{\mathbf{Exp}^{\text{SS-REAL}}_{\Sigma,C}(k)}$
$(prm, msk) \leftarrow S(1^k);$
$(id^*, s) \leftarrow C_1^{K(\,msk,\,\cdot\,)}(prm);$
$(ct, kem) \leftarrow E(prm, id^*);$
$v \leftarrow C_2^{K^{\{id^*\}}(msk,\cdot)}(ct, kem, s);$

$\underline{\mathbf{Exp}^{\text{SS-IDEAL}}_{\Sigma,\Sigma^*,C}(k)}$
$(prm, msk) \leftarrow S^*(1^k);$
$(id^*, s) \leftarrow C_1^{K^*(\,msk,\,\cdot\,)}(prm);$
$ct \leftarrow E^*(msk);\ kem' \leftarrow \mathcal{K};$
$v \leftarrow C_2^{K^*(\,msk,\,\cdot\,)}(ct, kem', s);$

In the above, $\mathcal{K}$ is a symmetric-key space. Key generation oracle $K(\,msk,\,\cdot\,)$ and simulator $K^*(\,msk,\,\cdot\,)$ get as input the msk and arbitrary $id \in \mathcal{ID}$, and output user secret key usk_{id} associated with id. C_1 cannot use id^* that is queried to KeyGen oracle as the target ID. If C_2 queries id^* to $K^{\{id^*\}}(msk, \cdot)$, $K^{\{id^*\}}(msk, \cdot)$ outputs $\perp$. At the end of the game, C_2 outputs a bit $v = \{0, 1\}$. We define the advantage $\mathbf{Adv}^{\text{Ano-SS}}_{\Sigma,\Sigma^*,A}(k)$ as follows

$$\mathbf{Adv}^{\text{SS}}_{\Sigma,\Sigma^*,C}(k) := |\Pr\left[\ \mathbf{Exp}^{\text{SS-REAL}}_{\Sigma,C}(k) \to 1\ \right] - \Pr\left[\ \mathbf{Exp}^{\text{SS-IDEAL}}_{\Sigma,\Sigma^*,C}(k) \to 1\ \right]|$$

Definition 3 (Ano-SS)**.** *We say that IB-KEM scheme $\Sigma = (S, K, E, D)$ is Ano-SS secure if for any PPT adversary $C = (C_1, C_2)$ there exists a PPT simulator $\Sigma^* = (S^*, K^*, E^*)$ such that $\mathbf{Adv}^{\text{Ano-SS}}_{\Sigma,\Sigma^*,C}(k)$ is negligible.*

In the above, C tries to guess whether it is in SS-REAL or SS-IDEAL from the information it obtains during the game. In SS-REAL, C gets (ct, kem) that is generated with respect to the challenge identity id^* chosen by C. In SS-IDEAL, C gets (ct, kem'), which is generated by the simulator E^* that does not see id^* at all. If C cannot distinguish SS-REAL from SS-IDEAL, it indicates that the information of id^* is not leaked to C.

3.2 Proof that Ano-SS Implies Ano-LOR

In this section we show that any Ano-SS secure IB-KEM is also Ano-LOR secure. The theorem and the proof is as follows.

Theorem 1. *If an IB-KEM scheme $\Sigma = (S, K, E, D)$ is Ano-SS secure, Σ is Ano-LOR secure.*

Proof. We will prove that if Σ is not Ano-LOR secure, then Σ is not Ano-SS secure. That is, we construct PPT adversary against Ano-SS security using PPT adversary against Ano-LOR security.

$B_1^{\mathcal{O}}(prm)$:
$(id_0, id_1, s) \leftarrow A_1^{K(\,msk,\,\cdot\,)}(prm)$
$b \leftarrow \{0,1\}$
output (id_b, s)

$B_2^{\mathcal{O}\{id_b\}}(ct, kem, s)$:
$b' \leftarrow A_2^{K\{id_0,id_1\}(msk,\cdot)}(ct, kem, s)$
If
$v := b'$
output v

Fig. 1. The construction of Ano-SS adversary $B = (B_1, B_2)$ using Ano-LOR adversary $A = (A_1, A_2)$.

$\mathbf{Exp}^{\text{SS-REAL}}_{\Sigma,B}$
$(msk, prm) \leftarrow S(1^k)$
$(id_b, s) \leftarrow B_1^{K(\,msk,\,\cdot\,)}(prm)$
$(ct, kem) \leftarrow E(id_b, prm)$
$v \leftarrow B_2^{K\{id_b\}(msk,\cdot)}(ct, kem, s)$

$\mathbf{Exp}^{\text{SS-IDEAL}}_{\Sigma,\Sigma^*,B}$
$(msk, prm) \leftarrow S^*(1^k)$
$(id_b, s) \leftarrow B_1^{K^*(\,msk,\,\cdot\,)}(prm)$
$(ct, kem) \leftarrow E^*(msk)$
$kem' \leftarrow \mathcal{K}$
$v \leftarrow B_2^{K^*\{id_b\}(msk,\cdot)}(ct, kem', s)$

Fig. 2. Adversary $B = (B_1, B_2)$ in the Ano-SS game.

Let $A = (A_1, A_2)$ be an arbitrary PPT adversary against the Ano-LOR security of Σ. The construction of PPT adversary $B = (B_1, B_2)$ against Ano-SS security using A is shown in Fig. 1.

In Fig. 1, $\mathcal{O}$ is key generation oracle, that takes msk and arbitrary $id' \in \mathcal{ID}$ as input and outputs $usk_{id'}$ associated with id'. When A queries id', B queries id' to $\mathcal{O}$ and return $usk_{id'}$ to A. In Fig. 2, we provide the description of the Ano-SS game with B.

Here, we discuss that if B is in the real game, B perfectly simulates the Ano-LOR game for A. First, we observe that any key query made by A is answered by B, who queries the same identity to $K(\,msk,\,\cdot\,)$ to obtain the secret key and passes it to A. Furthermore, B can answer any secret key query made by A because A is prohibited from making secret key query for id_0 or id_1 whereas B is prohibited the query only for id_b. Thus we have

$$\Pr[\mathbf{Exp}^{\text{SS-REAL}}_{\Sigma,B}(k) \to 1] = \Pr[b = b' | \mathbf{Exp}^{\text{LOR-}b}_{\Sigma,A}(k) \to b'].$$

Next, we will discuss the view of A in case B is in the ideal game. In this case, b is information theoretically hidden from A because (ct, kem) is generated by E^* that does not take id^* as input. Since b' is independent from b, we have

$$\Pr[\mathbf{Exp}^{\text{SS-IDEAL}}_{\Sigma,\Sigma^*,B}(k) \to 1] = \frac{1}{2}.$$

Finally, we have that

$$\begin{aligned}\mathbf{Adv}^{\mathrm{SS}}_{\Sigma,\Sigma^*,B}(k) &= |\Pr[\mathbf{Exp}^{\text{SS-REAL}}_{\Sigma,B}(k) \to 1] - \Pr[\mathbf{Exp}^{\text{SS-IDEAL}}_{\Sigma,\Sigma^*,B}(k) \to 1]| \\ &= |\Pr[b = b' | \mathbf{Exp}^{\mathrm{LOR}-b}_{\Sigma,A}(k) \to b'] - \frac{1}{2}| \\ &= \mathbf{Adv}^{\mathrm{LOR}}_{\Sigma,A}(k).\end{aligned}$$

Since A is the Ano-LOR adversary, $\mathbf{Adv}^{\mathrm{LOR}}_{\Sigma,A}(k)$ is a non-negligible. Hence, $\mathbf{Adv}^{\mathrm{SS}}_{\Sigma,\Sigma^*,B}(k)$ is also a non-negligible function.

From the above, it is true that if there is an Ano-LOR adversary A, then there is also an Ano-SS adversary B. Accordingly, if Σ is Ano-SS secure, then Σ is Ano-LOR secure. □

$S^*(1^k)$:
  $(prm, msk) \leftarrow S(1^k)$
  output (prm, msk)

$K^*(msk, id)$:
  $usk \leftarrow K(msk, id)$
  output usk

$E^*(msk)$:
  $id_1 \leftarrow \mathcal{ID}$
  $(ct, kem) \leftarrow E(id_1, prm)$
  output ct

Fig. 3. The construction of Σ^*.

4 Equivalence Between Ano-LOR and Ano-SS

In this section, we show that any Ano-LOR secure IB-KEM is also Ano-SS secure. Since we proved the other direction of the implication in Theorem 1, this implies that these two security notions are in fact equivalent.

As mentioned in the introduction, the security proof will be done by standard techniques with one exception. We elaborate on this in the following. In the security proof, we let the simulator generate a ciphertext for random identity. We then gradually change the game from the real game where the adversary is given a ciphertext corresponding to the identity chosen by itself to the ideal game where the ciphertext is chosen by the simulator. If our focus was on payload hiding, this change would be straightforward. However, our focus is on anonymity and this means that we have to come up with a reduction that abides by the restriction on key extraction queries, which is a challenge that is not present in the payload hiding settings. In particular, in order to invoke Ano-LOR security to prove indistinguishability between the real and ideal games, we have to make sure that the underlying Ano-SS adversary does not make a key extraction query for the random identity chosen by the simulator more than negligible probability,

even if it is given the ciphertext corresponding to that identity. This step cannot be done without computational assumption since the challenge ciphertext carries the information of the associated identity in information theoretic sense. Instead of information theoretic argument, we prove this by the additional invocation of Ano-LOR security.

The theorem and the proof is as follows. The proof will be done by considering sequence of games. While the changes from Game 0 to Game 3 are standard, the change from Game 3 to Game 4 requires more complicated argument reflecting the difficulty we outlined above.

Theorem 2. *If an IB-KEM scheme $\Sigma = (S, K, E, D)$ is Ano-LOR secure and IND-ID-CPA secure, then Σ is Ano-SS secure.*

Proof. Let $A = (A_1, A_2)$ be an arbitrary probabilistic polynomial-time adversary against the Ano-SS security of Σ. We construct a simulator $\Sigma^* = (S^*, E^*, K^*)$ satisfying $\mathbf{Adv}^{\mathrm{SS}}_{\Sigma,\Sigma^*,A}(k) \leq \varepsilon(k)$. The construction of Σ^* is shown in Fig. 3. The proof proceeds with a sequence of games. The description of the games is shown

Game 0:
$(prm, msk) \leftarrow S(1^k)$
$(id_0, s) \leftarrow A_1^{K(msk,\cdot)}(prm)$
$(ct, kem) \leftarrow E(prm, id_0)$
$v \leftarrow A_2^{K^{\{id_0\}}(msk,\cdot)}(ct, kem, s)$

Game 1:
$(prm, msk) \leftarrow S(1^k)$
$(id_0, s) \leftarrow A_1^{K(msk,\cdot)}(prm)$
$id_1 \leftarrow \mathcal{ID}$
$(ct, kem) \leftarrow E(prm, id_0)$
$v \leftarrow A_2^{K^{\{id_0,id_1\}}}(ct, kem, s)$

Game 2:
$(prm, msk) \leftarrow S(1^k)$
$(id_0, s) \leftarrow A_1^{K(msk,\cdot)}(prm)$
$id_1 \leftarrow \mathcal{ID}$
$(ct, kem) \leftarrow E(prm, id_1)$
$v \leftarrow A_2^{K^{\{id_0,id_1\}}(msk,\cdot)}(ct, kem, s)$

Game 3:
$(prm, msk) \leftarrow S(1^k)$
$(id_0, s) \leftarrow A_1^{K(msk,\cdot)}(prm)$
$id_1 \leftarrow \mathcal{ID}$
$(ct, kem) \leftarrow E(prm, id_1)$
$kem' \leftarrow \mathcal{K}$
$v \leftarrow A_2^{K^{\{id_0,id_1\}}(msk,\cdot)}(ct, kem', s)$

Game 4:
$(prm, msk) \leftarrow S^*(1^k)$
$(id_0, s) \leftarrow A_1^{K(msk,\cdot)}(prm)$
$ct \leftarrow E^*(msk)$
$kem' \leftarrow \mathcal{K}$
$v \leftarrow A_2^{K^{\{id_0\}}(msk,\cdot)}(ct, kem', s)$

Fig. 4. The sequence of games for the proof of the Ano-SS security.

in Fig. 4. In the description of the games, by $K^S(msk, \cdot)$ we denote the oracle that returns $K(msk, id)$ to the query id if $id \notin S$ and returns $\perp$ if $id \in S$.

In the following, let G_i be the event that the output v of the adversary A_2 is equal to 1. Since Game 0 is identical to the SS-REAL game, it holds that $\Pr[G_0] = \Pr[\mathbf{Exp}^{\text{SS-REAL}}_{\Sigma,A}(k) \to 1]$. Similarly, Game 4 is identical to the SS-IDEAL game, it also holds that $\Pr[G_4] = \Pr[\mathbf{Exp}^{\text{SS-IDEAL}}_{\Sigma,\Sigma^*,A}(k) \to 1]$. Due to the triangle inequality, it holds that $|\Pr[\mathbf{Exp}^{\text{SS-REAL}}_{\Sigma,A}(k) \to 1] - \Pr[\mathbf{Exp}^{\text{SS-IDEAL}}_{\Sigma,\Sigma^*,A}(k) \to 1]| \leq \sum_{i=0}^{3} |\Pr[G_i] - \Pr[G_{i+1}]|$.

We bound these terms by proving the following propositions. Let q be an upper bound on the number of the queries that A_1 and A_2 issue in total.

Proposition 1. *It holds that* $|\Pr[G_0] - \Pr[G_1]| \leq q/|\mathcal{ID}|$.

Proof (of Proposition 1). The games differ only when A_2 issues id_1 as a query to the oracle. Since the choice of id_1 is completely hidden from A_2 and is chosen uniformly random over $\mathcal{ID}$, the probability that $\mathcal{A}_2$ issues id_1 as an oracle query is at most that $q/|\mathcal{ID}|$. Hence due to the difference lemma [40], the proposition follows.

$B_1(prm)$:
$(id_0, s) \leftarrow A_1^{K(msk,\cdot)}(prm)$
$id_1 \leftarrow \mathcal{ID}$
output (id_0, id_1, s)

$B_2(ct, kem, s)$:
$v \leftarrow C^{K^{\{id_0,id_1\}}(msk,\cdot)}(ct, kem, s)$
output $b' \leftarrow v$

Fig. 5. The adversary $B = (B_1, B_2)$ for proving Proposition 2.

$B'_1(prm)$:
$(id_0, s) \leftarrow A_1^{K(msk,\cdot)}(prm)$
$id_1 \leftarrow \mathcal{ID}$
output (id_1, s)

$B'_2(ct, kem, s)$:
$v \leftarrow C^{K^{\{id_0,id_1\}}(msk,\cdot)}(ct, kem, s)$
output $b' \leftarrow v$

Fig. 6. The adversary $B' = (B'_1, B'_2)$ for proving Proposition 3.

Proposition 2. *There exists an adversary* $B = (B_1, B_2)$ *attacking the Ano-LOR security of* Σ *whose advantage satisfies* $|\Pr[G_1] - \Pr[G_2]| = \mathbf{Adv}^{\text{Ano-LOR}}_{\Sigma,B}(k)$.

Proof (of Proposition 2). We construct an adversary $B = (B_1, B_2)$ as in Fig. 5. The adversary B_2 is prohibited from obtaining a user secret key for id_0 and id_1, however, it is able to simulate the oracle for A_2, since for the oracle queries

id_0 or id_1 form A_2, it is sufficient to return $\perp$ to properly simulate the oracle $K^{\{id_0,id_1\}}(msk,\cdot)$. For the other oracle queries from A_2, it is sufficient to forward the queries to B_2's own oracle. Furthermore, if ct is an encapsulation with identity id_0, B perfectly simulates Game 1. Similarly, if ct is an encapsulation with identify id_1, B perfectly simulates Game 2. Therefore, it holds that

$$\begin{aligned}|\Pr[G_1] - \Pr[G_2]| &= |\Pr[\mathbf{Exp}^{\text{LOR-0}}_{\Sigma,B}(k) \to 1] - \Pr[\mathbf{Exp}^{\text{LOR-1}}_{\Sigma,B}(k) \to 1]| \\ &= \mathbf{Adv}^{\text{LOR}}_{\Sigma,B}(k),\end{aligned}$$

which proves the proposition.

Proposition 3. *There exists an adversary $B' = (B'_1, B'_2)$ attacking the IND-ID-CPA security of Σ whose advantage satisfies $|\Pr[G_2] - \Pr[G_3]| = \mathbf{Adv}^{\text{IND-ID-CPA}}_{\Sigma,B'}(k)$.*

Proof (of Proposition 3). We construct an adversary $B' = (B'_1, B'_2)$ as in Fig. 6. Similarly to the proof of Proposition 2, the adversary B'_2 is not allowed to obtain a user secret key for id_1. This does not cause B'_2's failure in simulating the oracle for A_2, because for A_2' query id_1 it is sufficient to responds with $\perp$. In addition, if kem is the real session key encapsulated in ct, B' perfectly simulates Game 2. Similarly, if kem is the random session key, B' perfectly simulates Game 3. Thus we have that

$$\begin{aligned}|\Pr[G_2] - \Pr[G_3]| &= |\Pr[\mathbf{Exp}^{\text{IND-ID-CPA-0}}_{\Sigma,B'}(k) \to 1] - \Pr[\mathbf{Exp}^{\text{IND-ID-CPA-1}}_{\Sigma,B'}(k) \to 1]| \\ &= \mathbf{Adv}^{\text{IND-ID-CPA}}_{\Sigma,B'}(k),\end{aligned}$$

which proves the proposition.

Game 3-1:	Game 3-2:
$(prm, msk) \leftarrow S(1^k)$	$(prm, msk) \leftarrow S(1^k)$
$(id_0, s) \leftarrow A_1^{K(msk,\cdot)}(prm)$	$(id_0, s) \leftarrow A_1^{K(msk,\cdot)}(prm)$
$id_1 \leftarrow \mathcal{ID}$	$id_1 \leftarrow \mathcal{ID}$
$id_2 \leftarrow \mathcal{ID}$	$id_2 \leftarrow \mathcal{ID}$
$(ct, kem) \leftarrow E(prm, id_1)$	$(ct, kem) \leftarrow E(prm, id_2)$
$kem' \leftarrow \mathcal{K}$	$kem' \leftarrow \mathcal{K}$
$v \leftarrow A_2^{K^{\{id_0,id_1,id_2\}}(prm,\cdot)}(ct, kem', s)$	$v \leftarrow A_2^{K^{\{id_0,id_1,id_2\}}(prm,\cdot)}(ct, kem', s)$

Fig. 7. The subsidiary games for proving Proposition 4.

$B_1''(prm)$:
$(id_0, s) \leftarrow A_1^{K(msk,\cdot)}(prm)$
$id_1 \leftarrow \mathcal{ID}$
$id_2 \leftarrow \mathcal{ID}$
output (id_1, id_2, s)

$B_2''(ct, kem, s)$:
$kem' \leftarrow \mathcal{K}$
$v \leftarrow A_2^{K^{\{id_0,id_1,id_2\}}(msk,\cdot)}(ct, kem', s)$
if id_1 is queried by A_2 then
$b' \leftarrow 1$
else
$b' \leftarrow 0$
output b'

Fig. 8. The adversary $B'' = (B_1'', B_2'')$ for proving Lemma 2.

Proposition 4. *There exists adversary* $\mathcal{B}'' = (B_1'', B_2'')$ *attacking the Ano-LOR security of* Σ *whose advantage satisfies* $|\Pr[G_3] - \Pr[G_4]| \leq 2q/|\mathcal{ID}| + \mathbf{Adv}^{\mathrm{LOR}}_{\Sigma,B''}(k)$.

Proof (of Proposition 4). Game 3 and 4 differ only when A_2 issues the oracle query id_1. Let us denote by F this event. Due to the difference lemma [40], we have that $|\Pr[G_3] - \Pr[G_4]| \leq \Pr[F]$. To bound the probability $\Pr[F]$, we introduce the following subsidiary sequence of games (Fig. 7). Let $F_{3\text{-}i}$ be the event that A_2 queries id_1 in Game 3-i. From the triangle inequality, we have that $\Pr[F] \leq |\Pr[F_3] - \Pr[F_{3\text{-}1}]| + |\Pr[F_{3\text{-}1}] - \Pr[F_{3\text{-}2}]| + \Pr[F_{3\text{-}2}]$. We bound these three terms in the following lemmas.

Lemma 1. *It holds that* $|\Pr[F_3] - \Pr[F_{3\text{-}1}]| \leq q/|\mathcal{ID}|$.

Proof (of Lemma 1). The games differ only when $\mathcal{A}_2$ issues the oracle query id_2. Since id_2 is completely hidden from A_2 and is chosen uniformly random over $\mathcal{ID}$, the probability that A_2 issues id_2 as an oracle query is at most $q/|\mathcal{ID}|$. Then, from the difference lemma [40], the lemma holds.

Lemma 2. *There exists an adversary* $B'' = (B_1'', B_2'')$ *attacking the IND-ID-CPA security of* Σ *whose advantage satisfies* $|\Pr[F_{3\text{-}1}] - \Pr[F_{3\text{-}2}]| = \mathbf{Adv}^{\text{IND-ID-CPA}}_{\Sigma,B''}(k)$.

Proof (of Lemma 2). We construct an adversary $B'' = (B_1'', B_2'')$ as in Fig. 8. The adversary B_2'' is not allowed to obtain a user secret key for id_1 and id_2. However, this does not cause B_2'''s failure of the simulation of the oracle $K^{\{id_0,id_1,id_2\}}(msk,\cdot)$, because for the oracle query id_1 and id_2 it is sufficient to respond with $\perp$. Moreover, if ct is an encapsulation with identity id_1, B'' perfectly simulates Game 3-1, and if ct is an encapsulation with identity id_2, B'' perfectly simulates Game 3-2. Furthermore, both in Game 3-1 and 3-2, if and only if A_2 queries id_1, namely, if and only if the event $F_{3\text{-}1}$ or $F_{3\text{-}2}$ occur, B_2'' outputs 1. Therefore, it holds that

$$\begin{aligned}
&|\Pr[F_{3\text{-}1}] - \Pr[F_{3\text{-}1}]| \\
&\quad = |\Pr[\mathbf{Exp}^{\text{LOR-0}}_{\Sigma,B''}(k) \to 1] - \Pr[\mathbf{Exp}^{\text{LOR-1}}_{\Sigma,B''}(k) \to 1]| \\
&\quad = \mathbf{Adv}^{\mathrm{LOR}}_{\Sigma,B''}(k),
\end{aligned}$$

which proves the lemma.

Lemma 3. *It holds that* $\Pr[F_{3\text{-}2}] \leq q/|\mathcal{ID}|$.

Proof (of Lemma 3). In Game 3-2, id_1 is completely hidden from A_2 and is chosen uniformly random over $\mathcal{ID}$. Thus the probability that A_2 issues the oracle query id_1 is at most $q/|\mathcal{ID}|$.

Lemmas 1, 2, and 3 show that $\Pr[F] \leq |\Pr[F_3] - \Pr[F_{3\text{-}1}]| + |\Pr[F_{3\text{-}1}] - \Pr[F_{3\text{-}2}]| + \Pr[F_{3\text{-}2}] \leq q/|\mathcal{ID}| + \mathbf{Adv}^{\mathrm{LOR}}_{\Sigma,B''}(k) + q/|\mathcal{ID}|$, which concludes the proof of the proposition.

Finally, combining all the propositions, we have that

$$\begin{aligned}\mathbf{Adv}^{\mathrm{SS}}_{\Sigma,\Sigma^*,A}(k) &= |\Pr[\mathbf{Exp}^{\text{SS-REAL}}(k) \to 1] - \Pr[\mathbf{Exp}^{\text{SS-IDEAL}}(k) \to 1]| \\ &\leq \frac{q}{|\mathcal{ID}|} + \mathbf{Adv}^{\mathrm{LOR}}_{\Sigma,B}(k) + \mathbf{Adv}^{\text{IND-ID-CPA}}_{\Sigma,B'}(k) + \frac{2q}{|\mathcal{ID}|} + \mathbf{Adv}^{\mathrm{LOR}}_{\Sigma,B''}(k).\end{aligned}$$

Since q is a polynomial of the security parameter k, and $|\mathcal{ID}|$ is exponential in k, then $q/|\mathcal{ID}|$ is negligible in k. Therefore, if Σ is Ano-LOR secure and IND-ID-CPA secure, then Σ is Ano-SS secure.

5 Discussion

In this section we discuss some theoretical and practical implications drawn from our results.

Equivalence of Simulation-Based and IND-Based Definitions. Firstly and obviously, our results claim that the IND-based definition is equivalent to the simulation-based definition for anonymity of IBE. This equivalence brings the following two desirable effects to the community. The first is that all the existing Ano-LOR secure IBE schemes are now automatically Ano-SS secure. Therefore, their anonymity becomes more reliable and theoretically well-founded all at once. The second is that if we want to design a new Ano-SS secure IBE scheme, it is sufficient to prove that a scheme is Ano-LOR secure. We notice that it eases the cost of providing a security proof, since the IND-based notion of Ano-LOR is easier to deal with than the simulation-based notion of Ano-SS. Nevertheless, our results ensure that a scheme which is proven Ano-LOR secure is also Ano-SS secure without any additional proofs.

Clarification of the Relation Between the Intuition and the Definition. Secondly, our results clarify the relationship between our intuition of anonymity and the security that is captured by Ano-LOR. As mentioned in the introduction, our Ano-SS notion captures the intuition that the recipient's ID is not leaked from a ciphertext more directly. In contrast to this, the Ano-LOR notion is designed analogously to the IND-CPA notion, which in turn results in an easier-to-deal-with but less intuitive notion. Filling this subtle gap between the two security notions, which has not been investigated more than 15 years, would improve our understanding on the security notions of IBE.

Potential Nontriviality in Proving Equivalence. Finally, our security proof suggests that we may encounter a situation where the IND-based notion is *not* equivalent to simulation-based notion depending on a cryptographic primitive in question. This is because in our security proof that Ano-LOR implies Ano-SS, there are several non-trivialities. For this nontriviality, we could not straightforwardly apply Goldwasser-Micali's technique [24] of proving the equivalence of an IND-based notion and a simulation-based notion.

This suggests that for more sophisticated primitives, there is possibility of not holding the equivalence between an IND-based secrecy notion and an simulation based one. Such a situation has already occurred in the context of functional encryption, where their IND-based and simulation-based notions are in fact *not* equivalent [11]. In addition, for selective-opening security of public-key encryption, the simulation-based security and the IND-based security do not imply each other [8]. For non-malleability of public-key encryption, there are variations of simulation-based definitions and IND-based definitions, and the relationships between them are quite complicated depending on whether the adversary has access to decryption oracle [36].

We conjecture that if the behavior of oracles and restriction on the adversary's queries become more and more complicated, it becomes more and more plausible to be unable to apply classical techniques to prove the equivalence between a simulation-based definition and an IND-based definition. We remark that the root of the non-triviality of our proof was the existence of *the key generation oracle*, which can be seen as an oracle with very basic type of functionality and it still brought an involved situation to the security game. Thus, it is important to study the equivalence between IND-based and simulation-based security notions for various cryptographic primitives, otherwise we may overlook a subtlety in the (in)equivalence between security notions of the different natures.

Other Studies that Rely on a Variant of Anonymity. As one possible application of our research, we mention that there are other studies on the security against key generation center (KGC) in IBE [16,21], which is a variant of the work on anonymity in IBE.

Chow [16] and Emura et al. [21] discuss the ciphertext anonymity against KGC to tackle the problem on the key escrow problem in IBE. If we try to discuss this idea formally, we need a security definition in which the ciphertext is anonymous, even if the master key is given to the malicious adversary. They discussed this problem based on IND-based ciphertext anonymity introduced by Chow [16].

As we have discussed in this paper, it would be desirable here as well if the relationship between IND-based security and SIM-based security are clarified so that we can better understand what the definition actually means.

Although our definition does not provide a definition capturing the situation that master key is given to adversary, we believe that our results are useful as first step in providing such a definition.

Acknowledgement. We would like to thank the reviewers of ESORICS 2020 and Sherman S. M. Chow for precious comments. A part of this work was supported by JSPS KAKENHI Grant Number 18K18055, JSPS KAKENHI Grant Number 19H01109, and JST CREST Grant Number JPMJCR19F6.

A Attempt to Define Anonymity Based on Goldwasser and Micali's Approach

Definition Based on Goldwasser-Micali [24]. Here, we briefly recall the notion of semantic security (SS) defined by Goldwasser and Micali [24]. We say that a PKE scheme satisfies SS if there exists a simulator that can simulate view for an adversary that is indistinguishable from that of the real world where the adversary chooses a message and is given a ciphertext that encrypts it and the simulator is not provided any information of the message. In this section, we attempt to define SS for anonymity of IB-KEM following their approach [24] and observe that there seems no straightforward way to do so.

Let $\Sigma = (S, K, E, D)$ be an IB-KEM scheme, and $C = (C_1, C_2)$ be a PPT adversary. We also let $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ be a simulator. We formulate Ano-SS as follows: if the game SS-REAL ($\mathbf{Exp}^{\text{SS-REAL}}_{\Sigma,C}(k)$) where the adversary receives the ciphertext and guesses the information of the identity and the game SS-IDEAL ($\mathbf{Exp}^{\text{SS-IDEAL}}_{\Sigma,\mathcal{S}}(k)$) where the simulator $\mathcal{S}$ generates a simulated ciphertext without receiving the identity, is indistinguishable, then the IB-KEM scheme is said to satisfy Ano-SS.

$\underline{\mathbf{Exp}^{\text{SS-REAL}}_{\Sigma,C}(k)}$
$(prm, msk) \leftarrow S(1^k);$
$((P, F), s) \leftarrow C_1^{K(msk,\cdot)}(prm);$
$id^* \leftarrow P(\mathcal{ID})$
$(ct, kem) \leftarrow E(prm, id^*);$
$v \leftarrow C_2^{K(msk,\cdot)}(ct, kem, s);$
$\beta := 1 \leftrightarrow v = F(id^*)$

$\underline{\mathbf{Exp}^{\text{SS-IDEAL}}_{\Sigma,\mathcal{S}}(k)}$
$(prm, msk) \leftarrow S(1^k);$
$((P, F), s) \leftarrow \mathcal{S}_1(prm);$
$id^* \leftarrow P(\mathcal{ID})$

$v \leftarrow \mathcal{S}_2(s);$
$\beta := 1 \leftrightarrow v = F(id^*)$

In the above, P and F are PPT algorithms. P samples id^* from the ID space $\mathcal{ID}$, and F outputs partial information of the input. Key generation oracle $K(msk, \cdot)$ in $\mathbf{Exp}^{\text{SS-REAL}}_{\Sigma,C}(k)$ gets as input msk and arbitrary $id \in \mathcal{ID}$, and outputs a user secret key usk_{id} associated with id. C_1 cannot use the challenge identity id^* that is queried to $K^{\{id^*\}}(msk, \cdot)$ as the target ID. We define $\mathbf{Adv}^{\text{SS}}_{\Sigma,C,\mathcal{S}}(k)$, the advantage of the Ano-SS adversary as follows

$$\mathbf{Adv}^{\text{SS}}_{\Sigma,C,\mathcal{S}}(k) := |\Pr[\mathbf{Exp}^{\text{SS-REAL}}_{\Sigma,C}(k) \to 1] - \Pr[\mathbf{Exp}^{\text{SS-IDEAL}}_{\Sigma,\mathcal{S}}(k) \to 1]|.$$

Definition 4. *We say that IB-KEM scheme $\Sigma = (S, K, E, D)$ is* Ano-SS *secure if for any PPT adversary $C = (C_1, C_2)$ there exists PPT simulator $\mathcal{S}$ such that $\mathbf{Adv}^{\text{Ano-SS}}_{\Sigma,C,\mathcal{S}}(k)$ is negligible.*

Discussion on Definition 4. As we discuss here, Definition 4 is an incomplete security definition since there is an adversary that trivially breaks the security. For example, let us assume that $K(msk, \cdot)$ returns the user secret key usk_{id^*} associated with id^* when id^* is queried to the key generation oracle. In this case, the adversary can decrypt (ct, kem) encrypted with respect to the target ID id^* using usk_{id^*} and the adversary can identify the target ID by seeing if the decryption result matches with kem. We then discuss whether the adversary can indeed get a secret key for id^* from the oracle, since this is a sufficient condition for the above attack to succeed. Recall that id^* is sampled from the ID space $\mathcal{ID}$ by the polynomial time algorithm P. If the total number of IDs that P can output is at most a polynomial size, C is in fact able to find id^* by brute force attack in polynomial time. For this reason, in order to make Definition 4 an achievable security definition, it is necessary to add some constraint on the adversary's behavior. However, with such a constraint, we do not know whether the security notion is still meaningful. For example, we can consider following constraints. However, all of them have problems as we explain below.

Prohibit queries on key generation oracle
As mentioned above, one of the trivial attacks is to query id^* on key generation oracle. If the user secret key usk_{id^*} is given to the adversary, it can learn the information of the target identity from it. To prevent this kind of attack, let us restrict the adversary so that it cannot make a key query for id^*. More concretely, let us consider an alternative security definition where key generation oracle $K(msk, \cdot)$ sends $\perp$ back to the adversary C_2 when it queries id^* to key generation oracle $K(msk, \cdot)$ in the SS-REAL environment. However, the adversary can learn the information of id^* from the fact that the user secret key query is prohibited for this particular identity.

Changing the sampling P settings
In the above discussion, it was assumed that the total number of ID that P will output is of polynomial size, and thus the above attack was possible. A natural approach to prevent the attack is to restrict the adversary C to output P such that the number of ID that P can output is exponential. In this case, it seems that there is no trivial attack on the security. However, this restriction is less general because we pose a strict restriction on the sampler chosen by the adversary and thus significantly narrow the class of adversaries we capture. Since the meaning of the definition is unclear, we do not take this approach either.

As we discussed above, we do not know of any natural restrictions on the adversary that makes the security notion natural and meaningful. Therefore, we do not adopt the approach by [24] for defining semantic security style notion of anonymity.

References

1. Abdalla, M., et al.: Searchable encryption revisited: consistency properties, relation to anonymous IBE, and extensions. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 205–222. Springer, Heidelberg (2005). https://doi.org/10.1007/11535218_13
2. Arasu, A., Eguro, K., Kaushik, R., Kossmann, D., Ramamurthy, R., Venkatesan, R.: A secure coprocessor for database applications. In: 23rd International Conference on Field programmable Logic and Applications (FPL 2013), Porto, Portugal, 2–4 September 2013, pp. 1–8. IEEE (2013)
3. Aroki Systems: End to End Encryption for Active Data. https://www.aroki.com
4. Asharov, G., Naor, M., Segev, G., Shahaf, I.: Searchable symmetric encryption: optimal locality in linear space via two-dimensional balanced allocations. In: Wichs, D., Mansour, Y. (eds.) STOC 2016, pp. 1101–1114. ACM (2016)
5. Asharov, G., Segev, G., Shahaf, I.: Tight tradeoffs in searchable symmetric encryption. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018. LNCS, vol. 10991, pp. 407–436. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-96884-1_14
6. Attrapadung, N., et al.: Relations among notions of security for identity based encryption schemes. In: Correa, J.R., Hevia, A., Kiwi, M. (eds.) LATIN 2006. LNCS, vol. 3887, pp. 130–141. Springer, Heidelberg (2006). https://doi.org/10.1007/11682462_16
7. Blazy, O., Brouilhet, L., Phan, D.H.: Anonymous identity based encryption with traceable identities. In: ARES 2019, pp. 13:1–13:10 (2019)
8. Böhl, F., Hofheinz, D., Kraschewski, D.: On definitions of selective opening security. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 522–539. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-30057-8_31
9. Boneh, D., Di Crescenzo, G., Ostrovsky, R., Persiano, G.: Public key encryption with keyword search. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 506–522. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24676-3_30
10. Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44647-8_13
11. Boneh, D., Sahai, A., Waters, B.: Functional encryption: definitions and challenges. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 253–273. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19571-6_16
12. Boneh, D., Waters, B.: Conjunctive, subset, and range queries on encrypted data. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 535–554. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-70936-7_29
13. Boyen, X., Waters, B.: Anonymous hierarchical identity-based encryption (without random oracles). In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 290–307. Springer, Heidelberg (2006). https://doi.org/10.1007/11818175_17
14. 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.) PKC 2009. LNCS, vol. 5443, pp. 196–214. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-00468-1_12
15. Cash, D., Tessaro, S.: The locality of searchable symmetric encryption. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 351–368. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55220-5_20

16. Chow, S.S.M.: Removing Escrow from identity-based encryption. In: Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 256–276. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-00468-1_15
17. Cocks, C.: An identity based encryption scheme based on quadratic residues. In: Honary, B. (ed.) Cryptography and Coding 2001. LNCS, vol. 2260, pp. 360–363. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45325-3_32
18. Crypteron: Crypteron introduces secure, searchable encryption. https://crypteron.com/blog/practical-searchable-encryption-and-security
19. Demertzis, I., Papadopoulos, D., Papamanthou, C.: Searchable encryption with optimal locality: achieving sublogarithmic read efficiency. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018. LNCS, vol. 10991, pp. 371–406. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-96884-1_13
20. Demertzis, I., Papamanthou, C.: Fast searchable encryption with tunable locality. In: Salihoglu, S., Zhou, W., Chirkova, R., Yang, J., Suciu, D. (eds.) Proceedings of the 2017 ACM International Conference on Management of Data, SIGMOD Conference 2017, Chicago, IL, USA, 14–19 May 2017, pp. 1053–1067. ACM (2017)
21. 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., Ryan, P.Y.A. (eds.) ESORICS 2019. LNCS, vol. 11736, pp. 113–133. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-29962-0_6
22. Fan, C., Tseng, Y.: Anonymous multi-receiver identity-based authenticated encryption with CCA security. Symmetry **7**(4), 1856–1881 (2015)
23. Gajek, S.: Dynamic symmetric searchable encryption from constrained functional encryption. In: Sako, K. (ed.) CT-RSA 2016. LNCS, vol. 9610, pp. 75–89. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-29485-8_5
24. Goldwasser, S., Micali, S.: Probabilistic encryption. J. Comput. Syst. Sci. **28**(2), 270–299 (1984)
25. Google: Encrypted BigQuery client. https://github.com/google/encrypted-bigquery-client
26. Grofig, P., et al.: Experiences and observations on the industrial implementation of a system to search over outsourced encrypted data. In: Katzenbeisser, S., Lotz, V., Weippl, E.R. (eds.) Sicherheit 2014: Sicherheit, Schutz und Zuverlässigkeit, Beiträge der 7. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), 19–21 März 2014, Wien, Österreich. LNI, vol. P-228, pp. 115–125. GI (2014). http://subs.emis.de/LNI/Proceedings/Proceedings228/article7.html
27. He, K., Weng, J., Liu, J., Liu, J.K., Liu, W., Deng, R.H.: Anonymous identity-based broadcast encryption with chosen-ciphertext security. In: AsiaCCS 2016, pp. 247–255 (2016)
28. Wee, H.: Attribute-hiding predicate encryption in bilinear groups, revisited. In: Kalai, Y., Reyzin, L. (eds.) TCC 2017. LNCS, vol. 10677, pp. 206–233. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70500-2_8
29. Ishai, Y., Kushilevitz, E., Lu, S., Ostrovsky, R.: Private large-scale databases with distributed searchable symmetric encryption. In: Sako, K. (ed.) CT-RSA 2016. LNCS, vol. 9610, pp. 90–107. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-29485-8_6
30. Izabachène, M., Pointcheval, D.: New anonymity notions for identity-based encryption. In: SCN 2008, pp. 375–391 (2008)
31. Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Smart, N. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 146–162. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-78967-3_9

32. Kurosawa, K., Ohtaki, Y.: How to update documents *verifiably* in searchable symmetric encryption. In: Abdalla, M., Nita-Rotaru, C., Dahab, R. (eds.) CANS 2013. LNCS, vol. 8257, pp. 309–328. Springer, Cham (2013). https://doi.org/10.1007/978-3-319-02937-5_17
33. Ma, X., Wang, X., Lin, D.: Anonymous identity-based encryption with identity recovery. In: Susilo, W., Yang, G. (eds.) ACISP 2018. LNCS, vol. 10946, pp. 360–375. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-93638-3_21
34. Microsoft SQL Server: Always Encrypted Database Engine. https://goo.gl/51LwQ9
35. Park, D.J., Kim, K., Lee, P.J.: Public key encryption with conjunctive field keyword search. In: Lim, C.H., Yung, M. (eds.) WISA 2004. LNCS, vol. 3325, pp. 73–86. Springer, Heidelberg (2005). https://doi.org/10.1007/978-3-540-31815-6_7
36. Pass, R., Shelat, A., Vaikuntanathan, V.: Relations among notions of non-malleability for encryption. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 519–535. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-76900-2_32
37. Popa, R.A., Redfield, C.M.S., Zeldovich, N., Balakrishnan, H.: CryptDB: processing queries on an encrypted database. Commun. ACM **55**(9), 103–111 (2012)
38. Sakai, R., Ohgishi, K., Kasahara, M.: Cryptosystems based on pairings. In: Proceedings of Symposium on Cryptography and Information Security, Japan (2000)
39. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985). https://doi.org/10.1007/3-540-39568-7_5
40. Shoup, V.: Sequences of games: a tool for taming complexity in security proofs. IACR Cryptology ePrint Archive 2004, p. 332 (2004). http://eprint.iacr.org/2004/332
41. StrongSalt: Introducing the First Privacy API. https://www.strongsalt.com
42. Tu, S., Kaashoek, M.F., Madden, S., Zeldovich, N.: Processing analytical queries over encrypted data. PVLDB **6**(5), 289–300 (2013). http://www.vldb.org/pvldb/vol6/p289-tu.pdf
43. Xu, P., Li, J., Wang, W., Jin, H.: Anonymous identity-based broadcast encryption with constant decryption complexity and strong security. In: AsiaCCS 2016, pp. 223–233 (2016)
44. Yoneyama, K., Kimura, S.: Verifiable and forward secure dynamic searchable symmetric encryption with storage efficiency. In: Qing, S., Mitchell, C., Chen, L., Liu, D. (eds.) ICICS 2017. LNCS, vol. 10631, pp. 489–501. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-89500-0_42