PAPER Special Section on Discrete Mathematics and Its Applications

Outsider-Anonymous Broadcast Encryption with Keyword Search: Generic Construction, CCA Security, and with Sublinear Ciphertexts

Keita EMURA[†,††a)], **Kaisei KAJITA**[†††], *and* **Go OHTAKE**[†††], *Members*

SUMMARY As a multi-receiver variant of public key encryption with keyword search (PEKS), broadcast encryption with keyword search (BEKS) has been proposed (Attrapadung et al. at ASIACRYPT 2006/Chatterjee-Mukherjee at INDOCRYPT 2018). Unlike broadcast encryption, no receiver anonymity is considered because the test algorithm takes a set of receivers as input and thus a set of receivers needs to be contained in a ciphertext. In this paper, we propose a generic construction of BEKS from anonymous and weakly robust 3-level hierarchical identity-based encryption (HIBE). The proposed generic construction provides outsider anonymity, where an adversary is allowed to obtain secret keys of outsiders who do not belong to the challenge sets, and provides sublinear-size ciphertext in terms of the number of receivers. Moreover, the proposed construction considers security against chosen-ciphertext attack (CCA) where an adversary is allowed to access a test oracle in the searchable encryption context. The proposed generic construction can be seen as an extension to the Fazio-Perera generic construction of anonymous broadcast encryption (PKC 2012) from anonymous and weakly robust identity-based encryption (IBE) and the Boneh et al. generic construction of PEKS (EUROCRYPT 2004) from anonymous IBE. We run the Fazio-Perera construction employs on the first-level identity and run the Boneh et al. generic construction on the second-level identity, i.e., a keyword is regarded as a second-level identity. The third-level identity is used for providing CCA security by employing one-time signatures. We also introduce weak robustness in the HIBE setting, and demonstrate that the Abdalla et al. generic transformation (TCC 2010/JoC 2018) for providing weak robustness to IBE works for HIBE with an appropriate parameter setting. We also explicitly introduce attractive concrete instantiations of the proposed generic construction from pairings and lattices, respectively.

key words: *broadcast encryption with keyword search, outsider anonymity, CCA security*

1. Introduction

Public key encryption with keyword search (PEKS) [1] is a searchable encryption in a public key setting. Let assume that a content and related keywords are encrypted and the ciphertexts are preserved on a cloud server. A receiver specifies a keyword kw to be searched, generates a trapdoor, and sends it to the cloud server. The cloud server runs the test algorithm and returns a ciphertext of a content containing kw to the receiver. As a multi-receiver variant of PEKS, Attrapadung et al. [2] introduced broadcast encryption with keyword search (BEKS) whose security is defined as a selective manner. Chatterjee and Mukherjee [3] proposed a BEKS scheme which is secure under the SXDH (Symmetric eXternal Diffie-Hellman) assumption and provides adaptive security. They also mentioned that the generic construction of Ambrona et al. [4] on [5] or on [6] also provide pairing-based BEKS constructions. Note that, in the BEKS syntax, the test algorithm takes a set of receivers in addition to a ciphertext and a trapdoor. Thus, a set of receivers needs to be contained in a ciphertext, and their BEKS constructions do not provide receiver anonymity, i.e., information about receivers is leaked[*]. Other multi-receiver variants of PEKS have also been proposed [7]–[13] to reduce the communication cost compared to the case that a PEKS scheme is separately run for each receiver. Though they considered keyword privacy where no information about keyword is revealed from ciphertexts, they did not consider receiver anonymity. Receiver anonymity is recognized as an important security requirement for preserving privacy in the broadcast encryption context, and several attempts have been considered [14]–[19].

Liu et al. introduced broadcast authenticated encryption with keyword search (BAEKS) [20] as a multi-receiver variant of public key authenticated encryption with keyword search (PAEKS) [21]–[26][**] with receiver anonymity, and proposed a pairing-based BAEKS scheme (in the random oracle model) with linear-size ciphertext in terms of the number of receivers. The anonymity is defined as a restricted manner where the challenge sets S_0^* and S_1^* are fixed during the setup phase and an adversary is not allowed to obtain the secret key of a receiver, i.e., no corruption is allowed. Mukherjee [27] proposed a BAEKS scheme providing statistical consistency where the advantage is negligible for all computationally unbounded adversaries. The security model for anonymity is restricted as in the Liu et al. model where no corruption is allowed. Emura [28] proposed a

Manuscript received September 11, 2023.
Manuscript revised December 23, 2023.
Manuscript publicized February 26, 2024.

[†] Kanazawa University, Kanazawa-shi, 920-1192 Japan.
[††] National Institute of Information and Communications Technology, Koganei-shi, 184-8795 Japan.
[†††] Science and Technology Research Laboratories, Japan Broadcasting Corporation, Tokyo, 157-8510 Japan.
a) E-mail: k-emura@se.kanazawa-u.ac.jp

DOI: 10.1587/transfun.2023DMP0003

[*] Note that Chatterjee and Mukherjee [3] called a BEKS scheme anonymous, if the challenge ciphertext hides associated challenge keyword.

[**] In PAEKS, the encryption algorithm takes a sender secret key (in addition to a receiver public key and a keyword) as input, and the trapdoor generation algorithm takes a sender public key (in addition to a receiver secret key and a keyword) as input. This setting allows us to prevent the keyword guessing attack. See [21]–[26] for details.

generic construction of BAEKS that provides linear-size ciphertext in terms of the number of receivers, and provides full anonymity where an adversary is allowed to obtain the secret keys of the receivers belonging to $S_0^* \cap S_1^*$. The building block is PAEKS providing ciphertext anonymity and consistency in a multi-receiver setting. The generic construction extends the Libert et al. generic construction of anonymous broadcast encryption [14]. The building block of the Libert et al. generic construction is (key-private and weakly robust) public key encryption (PKE) that allows us to employ PAEKS instead of the PKE. The linear-size ciphertext seems mandatory when full anonymity is required due to the analyses by Kiayias-Samari [18] and Kobayashi-Watanabe-Minematsu-Shikata [17][†].

The Fazio-Perera generic construction of anonymous broadcast encryption [15] provides outsider anonymity, where no information about a receiver is leaked from ciphertexts against outsiders, i.e., an adversary is allowed to obtain secret keys of outsiders who belong to neither S_0^* nor S_1^*. At the expense of a weak anonymity level, the Fazio-Perera generic construction provides sublinear-size ciphertext using the subset cover framework [29]. In this paper, we mainly focus on the complete subtree (CS) method. Fazio and Perera mentioned that outsider anonymity seems a natural relaxation, since often the contents of the communication already reveal something about the recipient set. Since a main usage of PEKS is that the cloud server returns a ciphertext of a content containing a keyword to the receiver, outsider anonymous BAEKS with sublinear-size ciphertext is effective to reduce the communication cost. However, employing the Fazio-Perera generic construction to BAEKS is left as an open problem in [28] due to the following reason: the building block of the Fazio-Perera generic construction is (anonymous and weakly robust) identity-based encryption (IBE) that prevents to directly employ PAEKS because PAEKS is not ID-based and does not provide a secret key derivation algorithm. Since BEKS [2], [3] or multi-receiver variants of PEKS [7]–[13] did not consider receiver anonymity, proposing an outsider anonymous BEKS (or multi-receiver variants of PEKS) with sublinear-size ciphertext is an important and interesting topic.

1.1 Our Contribution

In this paper, we propose a generic construction of outsider anonymous BEKS from anonymous and weakly robust 3-level hierarchical identity-based encryption (HIBE) and one-time signatures. Informally, outsider anonymity in the BEKS context means that no information about receivers is revealed from ciphertexts when an adversary is allowed to obtain secret keys of outsiders who belong to neither S_0^* nor S_1^*, and is allowed to obtain trapdoors of all receivers with the restriction that if the receivers belong to $S_0^* \cup S_1^*$, then $kw \notin \{kw_0^*, kw_1^*\}$ where kw_0^* and kw_1^* are challenge keywords. Moreover, the proposed construction considers security against chosen-ciphertext attack (CCA) where an adversary is allowed to access a test oracle. The proposed generic construction provides sublinear-size ciphertext in terms of the number of receivers. Technically, our generic construction can be seen as an extension to the Fazio-Perera generic construction of anonymous broadcast encryption from anonymous and weakly robust IBE [15] and the Boneh et al. generic construction of PEKS from anonymous IBE [1], where we run the Fazio-Perera construction employs on the first-level identity and run the Boneh et al. generic construction on the second-level identity, i.e., a keyword is regarded as a second-level identity. The third level is used for the Canetti-Halevi-Katz (CHK) transformation [30] for providing CCA security. We also introduce weak robustness in the HIBE setting, and demonstrate that the Abdalla et al. generic transformation for providing weak robustness to IBE [31], [32] works for HIBE with an appropriate parameter setting.

Instantiations. We can employ any anonymous HIBE schemes, e.g., HIBE from parings [33]–[35], [41], [42] or from lattices [36], [43]–[45] with a suitable one-time signature scheme. We convert HIBEs to provide weak robustness via the generic construction [31], [32] which is explained in Sect. 3. We explicitly give attractive concrete instantiations of the proposed generic construction from pairings and lattices, respectively, and give comparisons in Table 1.

- For pairing-based instantiations, we select the Ramanna-Sarkar (RS) HIBE scheme [33], the Langrehr-Pan (LP) HIBE scheme [34], and the Blazy-Kiltz-Pan (BKP) HIBE scheme [35] which are secure under the SXDH (Symmetric eXternal Diffie-Hellman) assumption[††].
- For lattice-based instantiations, we select the Agrawal-Boneh-Boyen (ABB) HIBE scheme [36] though it provides selective security. By using the transformation given by Boneh and Boyen (BB) [37], it can be converted to provide adaptive security in the random oracle model (ROM) (See Theorem 7.2 in the ePrint version [46]) by the process of hashing the identity ID with ROM before using ID. The BB transformation is briefly explained (in the case of IBE) as follows. In the initial phase, the simulator $\mathcal{B}$ picks $\mathsf{ID}^*_{\mathsf{sel}}$ as the challenge identity of the underlying selective secure IBE scheme. For the challenge identity $\mathsf{ID}^*_{\mathsf{ada}}$, $\mathcal{B}$ programs $\mathsf{ID}^*_{\mathsf{sel}} = H(\mathsf{ID}^*_{\mathsf{ada}})$ where H is modeled as

[†] As mentioned by Boneh et al. [1], PEKS implies a one-bit encryption scheme where for a plaintext $m \in \{0, 1\}$, a ciphertext of m is a PEKS ciphertext for the keyword m, and a decryption key is two trapdoors for the keywords 0 and 1, respectively. By using the transformation, a one-bit broadcast encryption scheme can be constructed from BAEKS. However, it is not clear whether the lower bound of the ciphertext size can be adopted in BAEKS. Especially, a secret key is required for encryption in BAEKS unlike to broadcast encryption. Thus, further analysis is required whether the linear-size ciphertext is mandatory when full anonymity is required in BAEKS, and we leave it as a future work of this paper.

[††] When the k-linear assumption is employed, we state it the SXDH assumption by setting $k = 1$ in Table 1.

Table 1 Comparison among multi-receiver variants of PEKS. Auth. stands for Authenticity where a sender secret key is required for encryption as in PAEKS. Let U be the set of all receivers and $S \subseteq U$ be a set of receivers specified in the encryption algorithm. We denote $N = |U|$, $|S| = N' \leq N$, and $R = |U| - |S|$. CT, ROM, and STD stand for ciphertext, random oracle model, and standard model, respectively. BDHSE, DLIN, BDHE, DDHI, MSE-DDH, DBDH, BDH, CODH, SXDH, LWE, and NCRHF stand for Bilinear Diffie-Hellman Summation Exponent, Decision LINear, Bilinear Diffie-Hellman Exponentiation, Decisional Diffie-Hellman Inverse, Multi-Sequence of Exponents Diffie-Hellman, Decisional Bilinear Diffie-Hellman, Bilinear Diffie-Hellman, Computational Oracle Diffie-Hellman, Symmetric eXternal Diffie-Hellman, Learning With Errors, and Near-Collision Resistant Hash Functions, respectively. CCA stands for chosen-ciphertext attack in the searchable encryption context where an adversary is allowed to access a test oracle. We omit complexity assumptions for one-time signatures.

Scheme	Anonymity	Auth.	CT Size	Assumption	ROM/STD	CCA
Ali et al. [13]	No	No	$O(1)$	BDHSE	ROM	No
Kiayias et al. [8]	No	No	$O(1)$	DLIN&BDHE&DDHI	STD	No
Jiang et al. [7]	No	No	$O(1)$	MSE-DDH	ROM	No
Chatterjee and Mukherjee [3]	No	No	$O(1)$	SXDH	STD	No
Liu et al. [20]	Restricted	Yes	$O(N')$	DBDH	ROM	No
Mukherjee [27]	Restricted	Yes	$O(N')$	Bilateral Matrix DH	STD	No
Emura [28]+QCZZ [21]	Full	Yes	$O(N')$	BDH&CODH	ROM	No
Emura [28]+Mukherjee [27]	Full	Yes	$O(N')$	Bilateral Matrix DH	STD	No
Ours+RS [33] or JP [34] or BKP [35]	Outsider	No	$O(R\log(N/R))$	SXDH	STD	Yes
Ours+ABB [36]+BB [37]	Outsider	No	$O(R\log(N/R))$	LWE	ROM	Yes
Ours+Y [38]+AET [39]	Outsider	No	$O(R\log(N/R))$	LWE	STD	Yes
Ours+JKN [40]+AET [39]	Outsider	No	$O(R\log(N/R))$	LWE&NCRHF	STD	Yes

a random oracle. $\mathcal{B}$ guesses $\mathsf{ID}^*_{\mathsf{ada}}$ with the probability at least $1/q_H$ where q_H is the number of random oracle queries. Because there are schemes that are secure in the ROM but insecure in the quantum random oracle model (QROM) [47], it would be better to show that the BB transformation works in the QROM setting. Unfortunately, this all-but-one programming does not work well in the QROM setting because a superposition of all the identities can be sent by a single query, and $\mathcal{B}$'s guessing fails with overwhelming probability. Thus, though we do not deny the possibility to prove that the BB transformation works in the QROM setting, we state the underlying HIBE scheme as ABB+BB and require ROM in Table 1. We remark that Zhandry [48] proved that the ABB HIBE scheme is secure in the QROM but still it is selectively secure. For giving lattice-based instantiations in the standard model, we pay attention to the fact that the size of keyword space can be regarded as a polynomial of a security parameter or keywords have low entropy[†], and selective security is sufficient for employing the CHK transformation. Thus, we can employ a 3-level HIBE scheme that satisfies adaptive security only for the first level and selective security for the other levels. Asano-Emura-Takayasu (AET) [39] introduced such 3-level HIBE schemes where the first level is either the Yamada IBE scheme [38] or the Jager-Kurek-Niehues (JKN) IBE scheme [40] which is adaptively secure, and other levels are selectively secure by appending a part of the selectively secure ABB IBE scheme. We can employ the Asano et al. HIBE schemes[††]. By employing state-of-the-art IBE schemes for the first level, we can construct BEKS schemes whose master public keys consist of only poly-log matrices in terms of the security parameter, as in [38], [40]. We state the underlying HIBE scheme as Y+AET or JKN+AET in Table 1. Though Cash et al. [44] proposed a lattice-based adaptively secure HIBE scheme in the standard model, the master public key size is proportional to the square of the security parameter. Moreover, though Singh et al. [49] proposed a lattice-based adaptively secure HIBE scheme in the standard model, the scheme achieves only bounded security in the sense that the size of a modulus q depends on the number of adversary's key extraction queries. Thus, we do not employ the Cash et al. HIBE scheme and the Singh et al. HIBE scheme as candidates of instantiations.

For comparison, we instantiated the generic construction of BAEKS [28] from the Qin-Cui-Zheng-Zheng (QCZZ) PAEKS scheme [21] and the Mukherjee PAEKS scheme (i.e., the Mukherjee BAEKS scheme [27] with the single receiver setting) as specified in [28], as pairing-based BAEKS instantiations. We remark that no lattice-based instantiation was given because the Cheng-Meng lattice-based PAEKS scheme [22] was not proven to provide ciphertext anonymity[†††], and thus it was not stated as the building

[†] This is a reason why the keyword guessing attack has been widely researched: an adversary $\mathcal{A}$, that has a trapdoor, generates a PEKS ciphertext for a keyword kw chosen by $\mathcal{A}$ and runs the test algorithm with the trapdoor. If the test algorithm outputs 1, then $\mathcal{A}$ can detect that kw is associated to the trapdoor. Otherwise, $\mathcal{A}$ selects other keyword. If the size of keyword space is relatively small or keywords have low entropy, then this keyword guessing attack is a real threat.

[††] Though Asano et al. did not formally mention that 3-level HIBE schemes are anonymous, they showed that an HIBE ciphertext is indistinguishable from random in their security proof.

[†††] In the security proof, they showed that almost all elements of ciphertext are indistinguishable from random which is sufficient to prove that no information of keyword is revealed from ciphertexts. However, an element is selected from receiver's public key related distribution. Thus, it is not clear whether the Cheng-Meng PAEKS scheme provides anonymity. We emphasize that Cheng and Meng did not claim that their scheme provides anonymity.

block. Though Yao et al. [26] proposed a lattice-based PAEKS scheme, they did not define consistency which is mandatory to instantiate the generic construction of BAEKS. Thus, we do not consider the Yao et al. scheme as a building block.

CPA Security. Though we focus on CCA security in this paper, BEKS providing outsider CPA anonymity, where no test oracle is defined, can be constructed generically from 2-level anonymous and weakly robust HIBE. Then, we can still employ the Asano et al. HIBE schemes by eliminating the third-level for lattice-based instantiations.

2. Preliminaries

2.1 One-Time Signatures

An one-time signature scheme OTS consists of $(\mathsf{OTS.KeyGen}, \mathsf{OTS.Sign}, \mathsf{OTS.Verify})$. The key generation algorithm $\mathsf{OTS.KeyGen}$ takes a security parameter λ as input, and outputs a verification key and a signing key $(\mathsf{vk}, \mathsf{sigk})$. The signing algorithm $\mathsf{OTS.Sign}$ takes sigk and a message $M \in \mathsf{SigMspace}$ as input, where $\mathsf{SigMspace}$ is a signed message space, and outputs a signature σ. The verification algorithm $\mathsf{OTS.Verify}$ takes vk, σ, and M as input, and outputs 0 or 1. We require the correctness holds where for any λ, $(\mathsf{vk}, \mathsf{sigk}) \leftarrow \mathsf{OTS.KeyGen}(1^\lambda)$, and $M \in \mathsf{SigMspace}$, $\mathsf{OTS.Verify}(\mathsf{vk}, \mathsf{OTS.Sign}(\mathsf{sigk}, M), M) = 1$ holds. Moreover, we require the strong existential unforgeability against adaptive chosen message attack (sEUF-CMA) holds: Let $\mathcal{A}$ be probabilistic polynomial-time (PPT) adversaries. Here, $(\mathsf{vk}, \mathsf{sigk}) \leftarrow \mathsf{OTS.KeyGen}(1^\lambda)$, $(\sigma^*, M^*) \leftarrow \mathcal{A}^{\mathsf{OTS.Sign}(\cdot)}(\mathsf{vk})$, and $\mathcal{A}$ is allowed to send a message M to the signing oracle $\mathsf{OTS.Sign}$ just once that returns $\sigma \leftarrow \mathsf{OTS.Sign}(\mathsf{sigk}, M)$. We say that OTS is sEUF-CMA secure if the advantage $\mathsf{Adv}^{\mathsf{sEUF\text{-}CMA}}_{\mathsf{OTS},\mathcal{A}}(\lambda) := \Pr[\mathsf{OTS.Verify}(\mathsf{vk}, \sigma^*, M^*) = 1 \wedge (\sigma^*, M^*) \neq (\sigma, M)]$ is negligible in the security parameter.

2.2 Anonymous 3-Level Hierarchical Identity-Based Encryption

Definition 1. *[Syntax of 3-level HIBE] An HIBE scheme* HIBE *consists of the following five algorithms* $(\mathsf{HIBE.Setup}, \mathsf{HIBE.KeyGen}, \mathsf{HIBE.KeyDer}, \mathsf{HIBE.Enc}, \mathsf{HIBE.Dec})$ *defined as follows. Here,* Mspace *is a message space and* $\mathsf{IDspace}$ *is an identity space. A hierarchical identity is denoted as* $(\mathsf{ID}, \mathsf{ID}', \mathsf{ID}'') \in \mathsf{IDspace} \times \mathsf{IDspace} \times \mathsf{IDspace}$*, and we consider the three-dimension identity only. In our purpose, it is sufficient that the* $\mathsf{HIBE.KeyGen}$ *algorithm generates a secret key for a first-level identity* ID *and the* $\mathsf{IBE.Enc}$ *algorithm takes a hierarchical identity* $(\mathsf{ID}, \mathsf{ID}', \mathsf{ID}'')$ *as input.*

$\mathsf{HIBE.Setup}$**:** *The setup algorithm takes a security parameter* λ *as input, and outputs a master public key* MPK *and a master secret key* MSK.

$\mathsf{HIBE.KeyGen}$**:** *The key generation algorithm takes* MPK, MSK*, and* $\mathsf{ID} \in \mathsf{IDspace}$ *as input, and outputs a secret key* $\mathsf{sk}_{\mathsf{ID}}$.

$\mathsf{HIBE.KeyDer}$**:** *For the second level key derivation, the key derivation algorithm takes* MPK, $\mathsf{sk}_{\mathsf{ID}}$*, and* $\mathsf{ID}' \in \mathsf{IDspace}$ *as input, and outputs a secret key* $\mathsf{sk}_{\mathsf{ID},\mathsf{ID}'}$*. For the third level key derivation, the key derivation algorithm takes* MPK, $\mathsf{sk}_{\mathsf{ID},\mathsf{ID}'}$*, and* $\mathsf{ID}'' \in \mathsf{IDspace}$ *as input, and outputs a secret key* $\mathsf{sk}_{\mathsf{ID},\mathsf{ID}',\mathsf{ID}''}$.

$\mathsf{HIBE.Enc}$**:** *The encryption algorithm takes* MPK, $(\mathsf{ID}, \mathsf{ID}', \mathsf{ID}'') \in \mathsf{IDspace} \times \mathsf{IDspace} \times \mathsf{IDspace}$*, and a plaintext* $M \in \mathsf{Mspace}$ *as input, and outputs a ciphertext* $\mathsf{ct}_{\mathsf{HIBE}}$.

$\mathsf{HIBE.Dec}$**:** *The decryption algorithm takes* MPK, $\mathsf{ct}_{\mathsf{HIBE}}$*, and* $\mathsf{sk}_{\mathsf{ID},\mathsf{ID}',\mathsf{ID}''}$ *as input, and outputs* M *or* $\perp$.

Correctness. For any security parameter λ, $(\mathsf{MPK}, \mathsf{MSK}) \leftarrow \mathsf{HIBE.Setup}(1^\lambda)$, $\mathsf{ID}, \mathsf{ID}', \mathsf{ID}'' \in \mathsf{IDspace}$, and $M \in \mathsf{Mspace}$, $\mathsf{HIBE.Dec}(\mathsf{MPK}, \mathsf{ct}_{\mathsf{HIBE}}, \mathsf{sk}_{\mathsf{ID},\mathsf{ID}',\mathsf{ID}''}) = M$ holds where $\mathsf{ct}_{\mathsf{HIBE}} \leftarrow \mathsf{HIBE.Enc}(\mathsf{MPK}, (\mathsf{ID}, \mathsf{ID}', \mathsf{ID}''), M)$, $\mathsf{sk}_{\mathsf{ID}} \leftarrow \mathsf{HIBE.KeyGen}(\mathsf{MPK}, \mathsf{MSK}, \mathsf{ID})$, $\mathsf{sk}_{\mathsf{ID},\mathsf{ID}'} \leftarrow \mathsf{HIBE.KeyDer}(\mathsf{MPK}, \mathsf{MSK}, \mathsf{sk}_{\mathsf{ID}}, \mathsf{ID}')$, and $\mathsf{sk}_{\mathsf{ID},\mathsf{ID}',\mathsf{ID}''} \leftarrow \mathsf{HIBE.KeyDer}(\mathsf{MPK}, \mathsf{MSK}, \mathsf{sk}_{\mathsf{ID},\mathsf{ID}'}, \mathsf{ID}'')$.

Anonymity. Briefly, anonymity means that no information about $(\mathsf{ID}, \mathsf{ID}', \mathsf{ID}'')$ is revealed from a ciphertext $\mathsf{ct}_{\mathsf{HIBE}} \leftarrow \mathsf{HIBE.Enc}(\mathsf{MPK}, (\mathsf{ID}, \mathsf{ID}', \mathsf{ID}''), M)$. The formal definition is as follows. We employ a CPA notion here.

Definition 2 (Anonymity)**.** *We define the following experiment.*

$$
\begin{aligned}
&\mathsf{Exp}^{\mathsf{Anon\text{-}CPA}\text{-}b}_{\mathsf{HIBE},\mathcal{A}}(\lambda):\\
&\quad (\mathsf{MPK}, \mathsf{MSK}) \leftarrow \mathsf{HIBE.Setup}(1^\lambda)\\
&\quad V_1 := \emptyset;\ V_2 := \emptyset;\ V_3 := \emptyset\\
&\quad ((\mathsf{ID}_0, \mathsf{ID}'_0, \mathsf{ID}''_0), (\mathsf{ID}_1, \mathsf{ID}'_1, \mathsf{ID}''_1), M^*_0, M^*_1, \mathsf{st})\\
&\qquad \leftarrow \mathcal{A}^{\mathsf{HIBE.KeyGen}(\mathsf{MPK},\mathsf{MSK},\cdot)}(\mathsf{MPK})\\
&\qquad \textit{s.t. } \mathsf{ID}_0, \mathsf{ID}_1 \notin V_1 \wedge (\mathsf{ID}_0, \mathsf{ID}'_0), (\mathsf{ID}_1, \mathsf{ID}'_1) \notin V_2\\
&\qquad \wedge (\mathsf{ID}_0, \mathsf{ID}'_0, \mathsf{ID}''_0), (\mathsf{ID}_1, \mathsf{ID}'_1, \mathsf{ID}''_1) \notin V_3\\
&\qquad \wedge M^*_0, M^*_1 \in \mathsf{Mspace} \wedge |M^*_0| = |M^*_1|\\
&\quad \mathsf{ct}^*_{\mathsf{HIBE}} \leftarrow \mathsf{HIBE.Enc}(\mathsf{MPK}, (\mathsf{ID}_b, \mathsf{ID}'_b, \mathsf{ID}''_b), M^*_b)\\
&\quad b' \leftarrow \mathcal{A}^{\mathsf{HIBE.KeyGen}(\mathsf{MPK},\mathsf{MSK},\cdot)}(\mathsf{ct}^*_{\mathsf{HIBE}}, \mathsf{st})\\
&\quad \textit{If } b = b'\textit{, then output } 1\textit{, and } 0 \textit{ otherwise.}
\end{aligned}
$$

The key extraction oracle $\mathsf{HIBE.KeyGen}$ *for the first-level identity takes* $\mathsf{ID} \in \mathsf{IDspace}$ *as input, returns* $\mathsf{sk}_{\mathsf{ID}} \leftarrow \mathsf{HIBE.KeyGen}(\mathsf{MSK}, \mathsf{ID})$*, and updates* $V_1 \leftarrow V_1 \cup \{\mathsf{ID}\}$*. The key extraction oracle* $\mathsf{HIBE.KeyGen}$ *for the two-dimensional hierarchical identities takes* $(\mathsf{ID}, \mathsf{ID}') \in \mathsf{IDspace} \times \mathsf{IDspace}$ *as input, computes* $\mathsf{sk}_{\mathsf{ID}} \leftarrow \mathsf{HIBE.KeyGen}(\mathsf{MSK}, \mathsf{ID})$*, returns* $\mathsf{sk}_{\mathsf{ID},\mathsf{ID}'} \leftarrow \mathsf{HIBE.KeyDer}(\mathsf{MSK}, \mathsf{sk}_{\mathsf{ID}}, \mathsf{ID}')$*, and updates* $V_2 \leftarrow V_2 \cup \{(\mathsf{ID}, \mathsf{ID}')\}$*. The key extraction oracle* $\mathsf{HIBE.KeyGen}$ *for the three-dimensional hierarchical identities takes* $(\mathsf{ID}, \mathsf{ID}', \mathsf{ID}'') \in \mathsf{IDspace} \times \mathsf{IDspace} \times \mathsf{IDspace}$ *as input, computes* $\mathsf{sk}_{\mathsf{ID}} \leftarrow \mathsf{HIBE.KeyGen}(\mathsf{MSK}, \mathsf{ID})$, $\mathsf{sk}_{\mathsf{ID},\mathsf{ID}'} \leftarrow \mathsf{HIBE.KeyDer}(\mathsf{MSK}, \mathsf{sk}_{\mathsf{ID}}, \mathsf{ID}')$*, returns* $\mathsf{sk}_{\mathsf{ID},\mathsf{ID}',\mathsf{ID}''} \leftarrow \mathsf{HIBE.KeyDer}(\mathsf{MSK}, \mathsf{sk}_{\mathsf{ID},\mathsf{ID}'}, \mathsf{ID}'')$*, and updates* $V_3 \leftarrow V_3 \cup \{(\mathsf{ID}, \mathsf{ID}', \mathsf{ID}'')\}$*. In the post-challenge phase, the oracle returns* $\perp$ *if any prefix of* $(\mathsf{ID}_0, \mathsf{ID}'_0, \mathsf{ID}''_0)$ *or*

$(\mathsf{ID}_1, \mathsf{ID}_1', \mathsf{ID}_1'')$ *is queried. We say that a HIBE scheme* HIBE *is Anon-CPA secure if the advantage* $\mathsf{Adv}^{\text{Anon-CPA}}_{\text{HIBE},\mathcal{A}}(\lambda) := |\Pr[\mathsf{Exp}^{\text{Anon-CPA-0}}_{\text{HIBE},\mathcal{A}}(\lambda) = 1] - \Pr[\mathsf{Exp}^{\text{Anon-CPA-1}}_{\text{HIBE},\mathcal{A}}(\lambda) = 1]|$ *is negligible for all PPT adversaries* $\mathcal{A}$ *in the security parameter* λ.

2.3 Complete Subtree Method

We introduce the complete subtree (CS) method [29]. Let BT be a binary tree with N leaves. For a leaf node i, let $\mathsf{Path}(i)$ be the set of nodes from the leaf to the root. Let RSet be the set of revoked leaves and $R = |\mathsf{RSet}|$. For non leaf node x, let x_{left} be the left child of x and x_{right} be the right child of x.

1. Initialize $X, \mathsf{cover} \leftarrow \emptyset$.
2. For all $i \in \mathsf{RSet}$, add $\mathsf{Path}(i)$ to X.
3. For all $x \in X$, if $x_{\mathsf{left}} \notin X$ then add x_{left} to cover. If $x_{\mathsf{right}} \notin X$ then add x_{right} to cover.
4. If $|\mathsf{Rset}| = 0$ then add the root node root to cover.
5. Output cover.

We denote $\mathsf{cover} \leftarrow \mathsf{CompSubTree}(\mathsf{BT}, \mathsf{RSet})$. $|\mathsf{cover}|$ is estimated as $O(R\log(N/R))^{\dagger}$.

2.4 Previous Generic Constructions

We briefly revisit previous generic constructions as follows.

The Abdalla et al. Generic Construction [52]. Abdalla et al. demonstrated that anonymous IBE implies PEKS. Briefly, a receiver runs $(\mathsf{MPK}, \mathsf{MSK}) \leftarrow \mathsf{IBE.Setup}(1^\lambda)$ and sets MPK as a public key and MSK as a secret key. To encrypt a keyword kw, a random plaintext R is encrypted using a keyword kw as the identity such that $\mathsf{ct}_{\mathsf{IBE}} \leftarrow \mathsf{IBE.Enc}(\mathsf{MPK}, kw, R)$ and $(\mathsf{ct}_{\mathsf{IBE}}, R)$ is a PEKS ciphertext. A trapdoor is a secret key $\mathsf{td}_{kw} \leftarrow \mathsf{IBE.KeyGen}(\mathsf{MSK}, kw)$. The test algorithm, that takes $(\mathsf{ct}_{\mathsf{IBE}}, R)$ and td_{kw} as input, outputs 1 if $R = \mathsf{IBE.Dec}(\mathsf{MPK}, \mathsf{ct}_{\mathsf{IBE}}, \mathsf{td}_{kw})$ and 0 otherwise. No information about kw is revealed from $(\mathsf{ct}_{\mathsf{IBE}}, R)$ if the underlying IBE scheme is anonymous. Moreover, if there exists kw' where $kw \neq kw'$ and the test algorithm outputs 1 for $\mathsf{td}_{kw'} \leftarrow \mathsf{IBE.KeyGen}(\mathsf{MSK}, kw')$ and $(\mathsf{ct}_{\mathsf{IBE}}, R)$ where $\mathsf{ct}_{\mathsf{IBE}} \leftarrow \mathsf{IBE.Enc}(\mathsf{MPK}, kw, R)$ (i.e., no consistency holds), then an algorithm can be constructed that breaks the IND-CPA security of the underlying IBE scheme. That is, the generic construction provides computational consistency.

The Boneh et al. Generic Construction [1]. The Boneh et al. generic construction is almost the same as the Abdalla et al. generic construction, except that R is fixed as 0^λ where $\lambda \in \mathbb{N}$ is a security parameter. $\mathsf{ct}_{\mathsf{IBE}}$ can be directly regarded as a PEKS ciphertext that reduces the ciphertext size compared to that of the Abdalla et al. generic construction. Abdalla et al. [52] showed that there is an IBE scheme that is anonymous and provides IND-CPA security, but the PEKS scheme obtained via the Boneh et al. generic construction does not provide consistency. Abdalla et al. also demonstrated that the Boneh et al. generic construction provides consistency if the underlying anonymous IBE is weakly robust [31], [32]. Briefly, robustness means that the decryption algorithm outputs $\perp$ if the corresponding decryption key is not used (See Sect. 3 for details). Abdalla et al. also mentioned that if the underlying IBE scheme is CCA secure in addition to provide weak robustness, then the PEKS scheme converted via the Boneh et al. generic construction is also CCA secure where an adversary is allowed to issue a test query.

The Fazio-Perera Generic Construction [15]. Fazio and Perera proposed a generic construction of anonymous broadcast encryption from anonymous IBE. Because the decryption algorithm does not take the set of receivers S as input, the underlying anonymous IBE scheme is required to be weakly robust. Let U be the set of all receivers and $S \subseteq U$ be a set of receivers specified in the encryption algorithm. We denote $N = |U|$, $R = |U| - |S|$, and $L = \lfloor R\log(N/R) \rfloor$. Moreover, let $\ell = |\mathsf{cover}|$ where $\mathsf{cover} = \{x_1, \dots, x_\ell\}$ is the set of nodes determined by the CS method. A ciphertext is a set of IBE ciphertexts: $\mathsf{ct}_{\mathsf{IBE},j} \leftarrow \mathsf{IBE.Enc}(\mathsf{MPK}, x_j, M)$ for $j = 1, 2, \dots, \ell$, and $\mathsf{ct}_{\mathsf{IBE},j} \leftarrow \mathsf{IBE.Enc}(\mathsf{MPK}, \mathsf{dummy}, \tilde{M})$ for $j = \ell+1, \dots, L$ where $\tilde{M} \xleftarrow{\$} \{0,1\}^{|M|}$ and dummy is a dummy identity. The order of ciphertexts is randomized via a random permutation. A receiver decrypts the ciphertext to find an IBE ciphertext whose decryption result is non-$\perp$. Due to the robustness of the underlying IBE scheme, a receiver can find such a ciphertext if the receiver belongs to the set S specified in the encryption algorithm. Due to the anonymity of the underlying IBE scheme, no information about identity is revealed from ciphertext in the sense of outsider anonymity. For providing CCA security, CCA secure anonymous IBE and one-time signatures are employed. A verification key vk is contained such that $\mathsf{ct}_{\mathsf{IBE},j} \leftarrow \mathsf{IBE.Enc}(\mathsf{MPK}, x_j, M||\mathsf{vk})$ for $j = 1, 2, \dots, \ell$, and $\mathsf{ct}_{\mathsf{IBE},j} \leftarrow \mathsf{IBE.Enc}(\mathsf{MPK}, \mathsf{dummy}, \tilde{M})$ for $j = \ell+1, \dots, L$ where $\tilde{M} \xleftarrow{\$} \{0,1\}^{|M|+|\mathsf{vk}|}$. A signature σ is generated on $\mathsf{vk}||\{\mathsf{ct}_{\mathsf{IBE},j}\}_{j\in[1,L]}$ and $(\sigma, \mathsf{vk}, \{\mathsf{ct}_{\mathsf{IBE},j}\}_{j\in[1,L]})$ is a ciphertext.

3. On Weak Robustness in the HIBE Setting

Briefly, robustness (in the HIBE setting) means that the HIBE.Dec algorithm that takes $\mathsf{ct}_{\mathsf{HIBE}}$ and $\mathsf{sk}_{\mathsf{ID}_1,\mathsf{ID}_1',\mathsf{ID}_1''}$ outputs an error symbol $\perp$ where $\mathsf{ct}_{\mathsf{HIBE}} \leftarrow \mathsf{HIBE.Enc}(\mathsf{MPK}, (\mathsf{ID}_0, \mathsf{ID}_0', \mathsf{ID}_0''), M)$, $\mathsf{sk}_{\mathsf{ID}_1} \leftarrow \mathsf{HIBE.KeyGen}(\mathsf{MPK}, \mathsf{MSK}, \mathsf{ID}_1)$, $\mathsf{sk}_{\mathsf{ID}_1,\mathsf{ID}_1'} \leftarrow \mathsf{HIBE.KeyDer}(\mathsf{MPK}, \mathsf{sk}_{\mathsf{ID}_1}, \mathsf{ID}_1')$, $\mathsf{sk}_{\mathsf{ID}_1,\mathsf{ID}_1',\mathsf{ID}_1''} \leftarrow \mathsf{HIBE.KeyDer}(\mathsf{MPK}, \mathsf{sk}_{\mathsf{ID}_1,\mathsf{ID}_1'}, \mathsf{ID}_1'')$, and $(\mathsf{ID}_0, \mathsf{ID}_0', \mathsf{ID}_0'') \neq (\mathsf{ID}_1, \mathsf{ID}_1', \mathsf{ID}_1'')$. Weak robustness here means that the robustness holds for honestly generated ciphertexts. The formal definition is as follows.

Definition 3 (Weak Robustness). *We define the following*

[†] More precisely, as mentioned in [50], [51], $|\mathsf{cover}|$ is estimated as $O(R\log(N/R))$ if $R \le N/2$ and is estimated as $O(N-R)$ if $N/2 < R \le N$. We assume that R is relatively smaller than N and then our construction provides sublinear-size ciphertext.

experiment.

```
$\mathsf{Exp}^{\mathsf{wrob}}_{\mathsf{HIBE},\mathcal{A}}(\lambda)$ :
    $(\mathsf{MPK}, \mathsf{MSK}) \leftarrow \mathsf{HIBE.Setup}(1^{\lambda})$
    $V := \emptyset$
    $((\mathsf{ID}_0, \mathsf{ID}'_0, \mathsf{ID}''_0), (\mathsf{ID}_1, \mathsf{ID}'_1, \mathsf{ID}''_1), M^*)$
      $\leftarrow \mathcal{A}^{\mathsf{HIBE.KeyGen}(\mathsf{MPK},\mathsf{MSK},\cdot)}(\mathsf{MPK})$
      $s.t.\ \mathsf{ID}_0, \mathsf{ID}_1 \notin V \wedge (\mathsf{ID}_0, \mathsf{ID}'_0, \mathsf{ID}''_0) \neq (\mathsf{ID}_1, \mathsf{ID}'_1, \mathsf{ID}''_1)$
      $\wedge\ M^* \in \mathsf{Mspace} \wedge M^* \neq \perp$
    $\mathsf{ct}_{\mathsf{HIBE}} \leftarrow \mathsf{HIBE.Enc}(\mathsf{MPK}, (\mathsf{ID}_0, \mathsf{ID}'_0, \mathsf{ID}''_0), M^*)$
    $\mathsf{sk}_{\mathsf{ID}_1} \leftarrow \mathsf{HIBE.KeyGen}(\mathsf{MPK}, \mathsf{MSK}, \mathsf{ID}_1)$
    $\mathsf{sk}_{\mathsf{ID}_1,\mathsf{ID}'_1} \leftarrow \mathsf{HIBE.KeyGen}(\mathsf{MPK}, \mathsf{sk}_{\mathsf{ID}_1}, \mathsf{ID}'_1)$
    $\mathsf{sk}_{\mathsf{ID}_1,\mathsf{ID}'_1,\mathsf{ID}''_1} \leftarrow \mathsf{HIBE.KeyGen}(\mathsf{MPK}, \mathsf{sk}_{\mathsf{ID}_1,\mathsf{ID}'_1}, \mathsf{ID}''_1)$
    If $\mathsf{HIBE.Dec}(\mathsf{MPK}, \mathsf{ct}_{\mathsf{HIBE}}, \mathsf{sk}_{\mathsf{ID}_1,\mathsf{ID}'_1,\mathsf{ID}''_1}) \neq \perp$,
    then output 1, and 0 otherwise.
```

The key extraction oracle HIBE.KeyGen *takes* $\mathsf{ID} \in \mathsf{IDspace}$ *as input, returns* $\mathsf{sk}_{\mathsf{ID}} \leftarrow \mathsf{HIBE.KeyGen}(\mathsf{MPK}, \mathsf{MSK}, \mathsf{ID})$*, and updates* $V \leftarrow V \cup \{\mathsf{ID}\}$. *We say that a HIBE scheme* HIBE *is weakly robust if the advantage* $\mathsf{Adv}^{\mathsf{wrob}}_{\mathsf{HIBE},\mathcal{A}}(\lambda) := \Pr[\mathsf{Exp}^{\mathsf{wrob}}_{\mathsf{HIBE},\mathcal{A}}(\lambda) = 1]$ *is negligible for all PPT adversaries* $\mathcal{A}$ *in the security parameter* λ.

The above definition follows that of Abdalla et al. that contains the key extraction oracle. We mention that the security of our generic construction holds even if the underlying HIBE scheme is weakly robust without the key extraction oracle.

Next, we demonstrate that the Abdalla et al. transformation [31], [32] works even for 3-level HIBE. Let $\mathsf{IDspace} = \{0,1\}^{\lambda}$ (basically, we assume that $\lambda = 128$ to provide 128-bit security level). For IBE[†], weak robustness can be easily obtained such that a random value $K \in \{0,1\}^{6\lambda}$ is chosen and is contained in MPK. For encryption of a plaintext M, $M||K$ is encrypted. The decryption algorithm outputs $\perp$ if K is not recovered, and M otherwise. Abdalla et al. required that K needs to be sufficiently larger than the identities because $\mathsf{Adv}^{\mathsf{wrob}}_{\mathsf{IBE},\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{Anon\text{-}CPA}}_{\mathsf{IBE},\mathcal{B}}(\lambda) + 2^{2|\mathsf{ID}|+\lceil \log_2(t) \rceil - |K|}$ holds (Theorem 4.1 in [31]), where $\mathcal{B}$ is an adversary for Anon-CPA security and t is the running time of an adversary of weak robustness $\mathcal{A}$. Abdalla et al. demonstrated a concrete example: assume $|\mathsf{ID}| = 256$ and $t \leq 2^{128}$, then $|K| = 768$ provides $2^{2|\mathsf{ID}|+\lceil \log_2(t) \rceil - |K|} = 2^{-128}$. Thus, we set $|K| = 6\lambda$ here.

We revisited the reason behind that K needs to be sufficiently larger than the identities. The reason is that an adversary (of weak robustness of IBE) can encode the key K into the identities ID_0 and ID_1. Then, there is an counterexample that the transformation fails to provide weak robustness. In the 3-level HIBE setting, an adversary can encode the key K into the hierarchical identities $(\mathsf{ID}_0, \mathsf{ID}'_0, \mathsf{ID}''_0)$ and $(\mathsf{ID}_1, \mathsf{ID}'_1, \mathsf{ID}''_1)$. Thus, the transformation still works when we set $|K| = 13\lambda$. The parameter selection is relatively conservative in the searchable encryption context. For example, if we assume that the size of keyword space is relatively small, then the identity-space of the second-level identities could be small, e.g., if we set $|\mathsf{KWspace}| = 2^{18}$ and $\lambda = 128$, then, $|\mathsf{KWspace}| \approx \lambda/7$ and $|K|$ could be estimated as $(4 + 2/7 + 4 + 1 + 1)\lambda \approx 10.3\lambda$[††]. We note that $|K|$ could be estimated as 6.3λ in the 2-level HIBE setting which is sufficient to construct BEKS with outsider CPA anonymity where no test oracle is defined.

4. Definition of BEKS

In this section, we introduce the definition of BEKS. We modify the definition of BAEKS [28]. Let N be the maximum number of receivers and $U = \{i\}_{i \in [1,N]}$ be the set of all receivers' indexes.

Definition 4 (Syntax of BEKS). *A BEKS scheme* BEKS *consists of the following four algorithms* (BEKS.Setup, BEKS.Enc, BEKS.Trapdoor, BEKS.Test) *defined as follows. Here,* KWspace *is a keyword space.*

- BEKS.Setup**:** *The setup algorithm takes a security parameter* λ *and the maximum number of receivers* N *as input, and outputs a master public key* MPK *and secret keys* $\{\mathsf{sk}_{\mathsf{R}[i]}\}_{i \in [1,N]}$. *Here,* R *stands for receiver and* $\mathsf{sk}_{\mathsf{R}[i]}$ *is a secret key of the* i*-th receiver.*
- BEKS.Enc**:** *The keyword encryption algorithm takes* MPK*, a set of receivers* $S \subseteq U$ *where* $|S| = N' \leq N$*, and a keyword* $kw \in \mathsf{KWspace}$ *as input, and outputs a ciphertext* $\mathsf{ct}_{\mathsf{BEKS}}$.
- BEKS.Trapdoor**:** *The trapdoor algorithm takes* MPK*,* sk_{R}*, and a keyword* $kw' \in \mathsf{KWspace}$ *as input, and outputs a trapdoor* $\mathsf{td}_{\mathsf{R},kw'}$.
- BEKS.Test**:** *The test algorithm takes* MPK*,* $\mathsf{ct}_{\mathsf{BEKS}}$ *and* $\mathsf{td}_{\mathsf{R},kw'}$ *as input, and outputs 1 or 0.*

Correctness. For any security parameter λ and $(\mathsf{MPK}, \{\mathsf{sk}_{\mathsf{R}[i]}\}_{i \in [1,N]}) \leftarrow \mathsf{BEKS.Setup}(1^{\lambda}, N)$, BEKS.Test $(\mathsf{MPK}, \mathsf{ct}_{\mathsf{BEKS}}, \mathsf{td}_{\mathsf{R},kw}) = 1$ holds where $\mathsf{ct}_{\mathsf{BEKS}} \leftarrow \mathsf{BEKS.Enc}(\mathsf{MPK}, S, kw)$, $\mathsf{td}_{\mathsf{R},kw} \leftarrow \mathsf{BEKS.Trapdoor}(\mathsf{MPK}, \mathsf{sk}_{\mathsf{R}[i]}, kw)$, $kw \in \mathsf{KWspace}$, and $i \in S \subseteq U$.

Consistency. We define consistency that basically requires that for any security parameter λ and $(\mathsf{MPK}, \{\mathsf{sk}_{\mathsf{R}[i]}\}_{i \in [1,N]}) \leftarrow \mathsf{BEKS.Setup}(1^{\lambda}, N)$, BEKS.Test $(\mathsf{MPK}, \mathsf{ct}_{\mathsf{BEKS}}, \mathsf{td}_{\mathsf{R},kw'}) = 0$ holds where $\mathsf{ct}_{\mathsf{BEKS}} \leftarrow \mathsf{BEKS.Enc}(\mathsf{MPK}, S, kw)$, $\mathsf{td}_{\mathsf{R},kw'} \leftarrow \mathsf{BEKS.Trapdoor}(\mathsf{MPK}, \mathsf{sk}_{\mathsf{R}[i]}, kw')$, and either $kw \neq kw'$ or $i \notin S$. We introduce computational consistency because the transformation for providing weak robustness [31], [32] assumes that the underlying IBE scheme is anonymous and IND-CPA secure.

Definition 5 (Computational Consistency). *We define the*

[†] Precisely, Abdalla et al. gave the transformation for general encryption that implies IBE and PKE.

[††] Oxford English Dictionary (the second edition of the 20-volume) contains 171,476 words. $2^{18} = 262,144$ can cover the number of words. See https://wordcounter.io/blog/how-many-words-are-in-the-english-language.

following experiment.

$\mathsf{Exp}^{\mathsf{consist}}_{\mathsf{BEKS},\mathcal{A}}(\lambda, N):$

$(\mathsf{MPK}, \{\mathsf{sk}_{\mathsf{R}[i]}\}_{i\in[1,N]}) \leftarrow \mathsf{BEKS.Setup}(1^\lambda, N)$

$(kw, kw', S^*, i^*) \leftarrow \mathcal{A}(\mathsf{MPK})$

s.t. $S^* \subseteq U \wedge i^* \in [1,N] \wedge kw, kw' \in \mathsf{KWspace}$

$\wedge\, (kw \neq kw' \vee i^* \notin S^*)$

$\mathsf{ct}_{\mathsf{BEKS}} \leftarrow \mathsf{BEKS.Enc}(\mathsf{MPK}, S^*, kw)$

$\mathsf{td}_{\mathsf{R},kw'} \leftarrow \mathsf{BEKS.Trapdoor}(\mathsf{MPK}, \mathsf{sk}_{\mathsf{R}[i^*]}, kw')$

If $\mathsf{BEKS.Test}(\mathsf{MPK}, \mathsf{ct}_{\mathsf{BEKS}}, \mathsf{td}_{\mathsf{R},kw'}) = 1,$

then output 1, *and* 0 *otherwise.*

We say that a BEKS scheme BEKS *is computationally consistent if the advantage* $\mathsf{Adv}^{\mathsf{consist}}_{\mathsf{BEKS},\mathcal{A}}(\lambda, N) := \Pr[\mathsf{Exp}^{\mathsf{consist}}_{\mathsf{BEKS},\mathcal{A}}(\lambda, N) = 1]$ *is negligible for all PPT adversaries* $\mathcal{A}$ *in the security parameter* λ.

Next, we introduce outsider anonymity, where an adversary $\mathcal{A}$ is allowed to obtain secret keys of outsiders who belong to neither S_0^* nor S_1^* via the corruption oracle, and is allowed to obtain trapdoors of all receivers via the trapdoor oracle with the restriction that if the receivers belong to $S_0^* \cup S_1^*$, then $kw \notin \{kw_0^*, kw_1^*\}$ where kw_0^* and kw_1^* are challenge keywords. We consider CCA security here where $\mathcal{A}$ is allowed to issue test queries $(i, kw, \mathsf{ct}_{\mathsf{BEKS}})$. If $i \in S_0^* \cup S_1^*$ and $\mathsf{ct}_{\mathsf{BEKS}} = \mathsf{ct}^*_{\mathsf{BEKS}}$, then $kw \notin \{kw_0^*, kw_1^*\}$ is required. If $S_0^* = S_1^*$, then the definition is the same as that of IND-CCA security. Thus, outsider CCA anonymity implies IND-CCA security.

Definition 6 (Outsider Anonymity). *We define the following experiment.*

$\mathsf{Exp}^{\mathsf{outsider\text{-}anon\text{-}}b}_{\mathsf{BEKS},\mathcal{A}}(\lambda, N):$

$(\mathsf{MPK}, \{\mathsf{sk}_{\mathsf{R}[i]}\}_{i\in[1,N]}) \leftarrow \mathsf{BEKS.Setup}(1^\lambda, N)$

$V := \emptyset;\ V' := \emptyset$

$(kw_0^*, kw_1^*, S_0^*, S_1^*, \mathsf{st})$

$\leftarrow \mathcal{A}^{\mathsf{BEKS.Trapdoor}(\cdot,\cdot),\mathsf{Corrupt}(\cdot),\mathsf{BEKS.Test}(\cdot,\cdot,\cdot)}(\mathsf{MPK})$

s.t. $S_0^*, S_1^* \subseteq U \wedge |S_0^*| = |S_1^*| \wedge V \cap (S_0^* \cup S_1^*) = \emptyset$

$\wedge\, kw_0^*, kw_1^* \in \mathsf{KWspace}$

$\wedge\, \forall (i, kw) \in V',$

$(i \notin S_0^* \cup S_1^* \wedge kw \in \mathsf{KWspace})$

$\vee\, (i \in S_0^* \cup S_1^* \wedge kw \in \mathsf{KWspace} \setminus \{kw_0^*, kw_1^*\})$

$\mathsf{ct}^*_{\mathsf{BEKS}} \leftarrow \mathsf{BEKS.Enc}(\mathsf{MPK}, S_b^*, kw_b^*)$

$b' \leftarrow \mathcal{A}^{\mathsf{BEKS.Trapdoor}(\cdot,\cdot),\mathsf{Corrupt}(\cdot),\mathsf{BEKS.Test}(\cdot,\cdot,\cdot)}(\mathsf{ct}^*_{\mathsf{BEKS}}, \mathsf{st})$

If $b = b'$, *then output* 1, *and* 0 *otherwise.*

Here, the trapdoor oracle BEKS.Trapdoor *takes* $i \in [1,N]$ *and* $kw \in \mathsf{KWspace}$, *returns the trapdoor generated as* $\mathsf{td}_{\mathsf{R},kw} \leftarrow \mathsf{BEKS.Trapdoor}(\mathsf{MPK}, \mathsf{sk}_{\mathsf{R}[i]}, kw)$, *and updates* $V' := V' \cup \{(i, kw)\}$. *In the post-challenge phase, the oracle returns* $\perp$ *if* $i \in S_0^* \cup S_1^*$ *and* $kw \in \{kw_0^*, kw_1^*\}$. *The corruption oracle* Corrupt *takes* $i \in [1,N]$ *as input, returns* $\mathsf{sk}_{\mathsf{R}[i]}$, *and updates* $V \leftarrow V \cup \{i\}$. *In the post-challenge phase, the oracle returns* $\perp$ *if* $i \in S_0^* \cup S_1^*$. *The test oracle* BEKS.Test *takes* $(i, kw, \mathsf{ct}_{\mathsf{BEKS}})$ *as input where* $i \in [1,N]$ *and* $kw \in \mathsf{KWspace}$, *computes* $\mathsf{td}_{\mathsf{R},kw} \leftarrow \mathsf{BEKS.Trapdoor}(\mathsf{MPK}, \mathsf{sk}_{\mathsf{R}[i]}, kw)$, *and returns the result of* $\mathsf{BEKS.Test}(\mathsf{MPK}, \mathsf{ct}_{\mathsf{BEKS}}, \mathsf{td}_{\mathsf{R},kw})$. *The oracle returns* $\perp$ *if* $i \in S_0^* \cup S_1^*$, $kw \in \{kw_0^*, kw_1^*\}$, *and* $\mathsf{ct}_{\mathsf{BEKS}} = \mathsf{ct}^*_{\mathsf{BEKS}}$. *We say that a BEKS scheme* BEKS *is outsider anonymous if the advantage* $\mathsf{Adv}^{\mathsf{outsider\text{-}anon}}_{\mathsf{BEKS},\mathcal{A}}(\lambda, N) := |\Pr[\mathsf{Exp}^{\mathsf{outsider\text{-}anon\text{-}0}}_{\mathsf{BEKS},\mathcal{A}}(\lambda, N) = 1] - \Pr[\mathsf{Exp}^{\mathsf{outsider\text{-}anon\text{-}1}}_{\mathsf{BEKS},\mathcal{A}}(\lambda, N) = 1]|$ *is negligible for all PPT adversaries* $\mathcal{A}$ *in the security parameter* λ.

5. Proposed Generic Construction

In this section, we give the proposed generic construction of BEKS from 3-level anonymous and weakly robust HIBE. Let U be the set of all receivers and $S \subseteq U$ be a set of receivers specified in the encryption algorithm. We denote $N = |U|$, $R = |U| - |S|$, and $L = \lfloor R \log(N/R) \rfloor$. Moreover, let $\ell = |\mathsf{cover}|$ where $\mathsf{cover} = \{x_1, \ldots, x_\ell\}$ is the set of nodes determined by the CS method, and BT be a binary tree with N leaves (i.e., assume that N is represented as 2^n for some $n \in \mathbb{N}$). Let dummy and dummy′ be dummy identities.

If we directly employ the Abdalla et al. generic construction [52], then a random plaintext R is contained in a BEKS ciphertext and it increases the ciphertext size. Here, we pay attention to the fact that the Fazio-Perera generic construction of anonymous broadcast encryption [15] requires that the underlying IBE scheme is weakly robust. Thus, we employ the Boneh et al. generic construction of PEKS [1] here that reduces the ciphertext size.

5.1 A Trivial Construction from IBE and Its Limitation

Before giving the proposed construction, we consider to directly employ the Boneh et al. generic construction of PEKS and discuss its limitation. For the sake of simplicity, we consider CPA security here where no test oracle is defined. Let $\mathsf{IBE} = (\mathsf{IBE.Setup}, \mathsf{IBE.KeyGen}, \mathsf{IBE.Enc}, \mathsf{IBE.Dec})$ be an IBE scheme. In the Boneh et al. construction, a receiver runs $(\mathsf{MPK}, \mathsf{MSK}) \leftarrow \mathsf{IBE.Setup}(1^\lambda)$ and MSK is used for generating a trapdoor by spesifying a keyword as the identity. Thus, a direct construction is described as follows. The BEKS.Setup algorithm runs $(\mathsf{MPK}_j, \mathsf{MSK}_j) \leftarrow \mathsf{IBE.Setup}(1^\lambda)$ for $j = 1, \ldots, N$, and outputs $\mathsf{MPK} = \{\mathsf{MPK}_j\}_{j\in[1,N]}$ and $\{\mathsf{sk}_{\mathsf{R}[j]} = \mathsf{MSK}_j\}_{j\in[1,N]}$. The BEKS.Enc algorithm, that takes $S \subseteq U$ where $|S| = N'$, specifies $\mathsf{RSet} := U \setminus S$ and runs $\mathsf{cover} \leftarrow \mathsf{CompSubTree}(\mathsf{BT}, \mathsf{RSet})$ where $\mathsf{cover} = \{x_1, \ldots, x_\ell\}$. Then, the algorithm runs $\mathsf{ct}_{\mathsf{IBE},j} \leftarrow \mathsf{IBE.Enc}(\mathsf{MPK}_j, x_j || kw, 0^\lambda)$ for $j = 1, 2, \ldots, \ell$, runs $\mathsf{ct}_{\mathsf{IBE},j} \leftarrow \mathsf{IBE.Enc}(\mathsf{MPK}_j, \mathsf{dummy}, \tilde{M})$ for $j = \ell + 1, \ldots, L$ where $\tilde{M} \xleftarrow{\$} \{0,1\}^\lambda$, and outputs $\mathsf{ct}_{\mathsf{BEKS}} = \{\mathsf{ct}_{\mathsf{IBE},\pi(j)}\}_{j\in[1,L]}$ where $\pi : \{1, \ldots, L\} \to \{1, \ldots, L\}$ is a random permutation. The BEKS.Trapdoor algorithm runs $\mathsf{sk}_k \leftarrow \mathsf{IBE.KeyGen}(\mathsf{MSK}_i, x'_k || kw')$ for $k = 1, \ldots, h$ where the receiver i is assigned to the leaf node i and $\mathsf{Path}(i) =$

$\{x'_1,\dots,x'_h\}$. Output $\mathsf{td}_{\mathsf{R},kw'} = (i,\{\mathsf{sk}_k\}_{k\in[1,h]})$. Then, the $\mathsf{BEKS.Test}$ algorithm, that takes $\mathsf{MPK} = \{\mathsf{MPK}_j\}_{j\in[1,N]}$, $\mathsf{ct}_{\mathsf{BEKS}} = \{\mathsf{ct}_{\mathsf{IBE},j}\}_{j\in[1,L]}$, and $\mathsf{td}_{\mathsf{R},kw'} = (i,\{\mathsf{sk}_k\}_{k\in[1,h]})$, runs:

```
• For $k = 1$ to $h$
    – For $j = 1$ to $L$
        ∗ Run $M \leftarrow \mathsf{IBE.Dec}(\mathsf{MPK}_i, \mathsf{ct}_{\mathsf{IBE},j}, \mathsf{sk}_k)$.
        ∗ If $M = 0^\lambda$, then return 1. Otherwise, if $j = L$,
          break the loop. Otherwise, $j \leftarrow j + 1$.
    – If $k = h$, return 0. Otherwise, $k \leftarrow k + 1$.
```

If $i \in S$, then $\mathsf{cover} \cap \mathsf{Path}(i) \neq \emptyset$ due to the CS method. Let $x_j \in \mathsf{cover} \cap \mathsf{Path}(i)$. If $kw = kw'$, then for $\mathsf{ct}_{\mathsf{BEKS}} \ni \mathsf{ct}_{\mathsf{IBE}} \leftarrow \mathsf{IBE.Enc}(\mathsf{MPK}_i, x_j||kw, 0^\lambda)$ and $\mathsf{td}_{\mathsf{R},kw'} \ni \{\mathsf{sk}_k\}_{k\in[1,h]} \ni \mathsf{sk} \leftarrow \mathsf{IBE.KeyGen}(\mathsf{sk}_{\mathsf{R}[i]}, x_j||kw')$, $0^\lambda \leftarrow \mathsf{IBE.Dec}(\mathsf{MPK}_i, \mathsf{ct}_{\mathsf{IBE}}, \mathsf{sk})$ holds. Thus, correctness directly holds due to the correctness of the underlying IBE scheme. Since the construction is almost the same as the Fazio-Perera construction, except that a keyword is appended to each node, the construction provides outsider anonymity. Moreover, due to the anonymity of the underlying IBE scheme, no information about keyword is revealed. However, to provide consistency, this construction requires the following robustness: for $\mathsf{ct}_{\mathsf{IBE}} \leftarrow \mathsf{IBE.Enc}(\mathsf{MPK}_i, \mathsf{ID}, M)$ and $\mathsf{sk}_{\mathsf{ID}'} \leftarrow \mathsf{IBE.KeyGen}(\mathsf{MPK}_j, \mathsf{MSK}_j, \mathsf{ID}')$, $\mathsf{IBE.Dec}(\mathsf{MPK}_j, \mathsf{ct}_{\mathsf{IBE}}, \mathsf{sk}_{\mathsf{ID}'}) = \perp$ holds if *not only the case* $\mathsf{ID} \neq \mathsf{ID}'$ *but also the case* $\mathsf{MPK}_i \neq \mathsf{MPK}_j$. This robustness *across the different master public keys* is not directly provided even if the underlying IBE scheme is robust.

5.2 Our Construction

Next, we give the proposed generic construction. To employ a single master public key, we employ HIBE in the proposed construction where a keyword is regarded as a second-level identity and a trapdoor is generated by using the key derivation algorithm of the underlying HIBE scheme.

For Providing CCA Security. As mentioned in Sect. 2.4, the Fazio-Perera generic construction provides CCA security (in the broadcast encryption context) if the underlying IBE scheme is CCA secure. Note that they employ a one-time signature scheme in addition to employ IBE because a set of IBE ciphertexts $\{\mathsf{ct}_{\mathsf{IBE},j}\}_{j\in[1,L]}$ is malleable (e.g., by a simple permutation) even if an IBE ciphertext $\mathsf{ct}_{\mathsf{IBE},j}$ is non-malleable due to the CCA security. That is, a verification key vk is contained as $\mathsf{ct}_{\mathsf{IBE},j} \leftarrow \mathsf{IBE.Enc}(\mathsf{MPK}, x_j, M||\mathsf{vk})$ for $j = 1, 2, \dots, \ell$, and $\mathsf{ct}_{\mathsf{IBE},j} \leftarrow \mathsf{IBE.Enc}(\mathsf{MPK}, \mathsf{dummy}, \tilde{M})$ for $j = \ell+1, \dots, L$ where $\tilde{M} \xleftarrow{\$} \{0,1\}^{|M|+|\mathsf{vk}|}$. A signature σ is generated on $\mathsf{vk}||\{\mathsf{ct}_{\mathsf{IBE},j}\}_{j\in[1,L]}$ and $(\sigma, \mathsf{vk}, \{\mathsf{ct}_{\mathsf{IBE},j}\}_{j\in[1,L]})$ is a ciphertext.

By using the Fazio-Perera methodology, one direct BEKS construction is: (1) construct a CCA secure 2-level HIBE from 3-level HIBE and one-time signatures via the CHK transformation, (2) convert the 2-level HIBE to be weakly robust, and (3) construct a CCA secure BEKS from the 2-level HIBE and one-time signatures via the Fazio-Perera methodology. However, one-time signatures are employed twice for providing CCA security for HIBE and for BEKS, respectively. For providing more efficient construction, we employ 3-level CPA secure HIBE and one-time signatures and directly construct BEKS that employs one-time signatures once.

The Proposed Generic Construction

$\mathsf{BEKS.Setup}(1^\lambda, N)$: Run $(\mathsf{MPK}', \mathsf{MSK}) \leftarrow \mathsf{HIBE.Setup}(1^\lambda)$. For $j = 1, \dots, N$, let $\mathsf{Path}(j) = \{x'_1, \dots, x'_h\}$ where h is the depth of BT and $x'_1 = \mathsf{root}$. For $k = 1, \dots, h$, run $\mathsf{sk}_k^{(j)} \leftarrow \mathsf{HIBE.KeyGen}(\mathsf{MSK}, x'_k)$. Output $\mathsf{MPK} = (\mathsf{MPK}', N)$ and $\{\mathsf{sk}_{\mathsf{R}[j]}\}_{j\in[1,N]}$ where $\mathsf{sk}_{\mathsf{R}[j]} = \{\mathsf{sk}_k^{(j)}\}_{k\in[1,h]}$. Here, $\mathsf{KWspace} = \mathsf{IDspace}$.[†]

$\mathsf{BEKS.Enc}(\mathsf{MPK}, S, kw)$: Parse $\mathsf{MPK} = (\mathsf{MPK}', N)$. Run $(\mathsf{vk}, \mathsf{sigk}) \leftarrow \mathsf{OTS.KeyGen}(1^\lambda)$. Specify $\mathsf{RSet} := U \setminus S$ and run $\mathsf{cover} \leftarrow \mathsf{CompSubTree}(\mathsf{BT}, \mathsf{RSet})$ where $\mathsf{cover} = \{x_1, \dots, x_\ell\}$. For $j = 1, \dots, \ell$, run $\mathsf{ct}_{\mathsf{HIBE},j} \leftarrow \mathsf{HIBE.Enc}(\mathsf{MPK}', (x_j, kw, \mathsf{vk}), 0^\lambda)$. For $j = \ell+1, \dots, L$, run $\mathsf{ct}_{\mathsf{HIBE},j} \leftarrow \mathsf{HIBE.Enc}(\mathsf{MPK}', (\mathsf{dummy}, \mathsf{dummy}', \mathsf{vk}), \tilde{M})$ where $\tilde{M} \xleftarrow{\$} \{0,1\}^\lambda$. Run $\sigma \leftarrow \mathsf{OTS.Sign}(\mathsf{sigk}, \{\mathsf{ct}_{\mathsf{HIBE},\pi(j)}\}_{j\in[1,L]})$ where $\pi : \{1, \dots, L\} \to \{1, \dots, L\}$ is a random permutation. Output $\mathsf{ct}_{\mathsf{BEKS}} = (\mathsf{vk}, \sigma, \{\mathsf{ct}_{\mathsf{HIBE},\pi(j)}\}_{j\in[1,L]})$.

$\mathsf{BEKS.Trapdoor}(\mathsf{MPK}, \mathsf{sk}_\mathsf{R}, kw')$: Parse $\mathsf{MPK} = (\mathsf{MPK}', N)$. Assume that the receiver is assigned to the leaf node i and $\mathsf{sk}_\mathsf{R} = \mathsf{sk}_{\mathsf{R}[i]}$. Parse $\mathsf{sk}_{\mathsf{R}[i]} = \{\mathsf{sk}_k^{(i)}\}_{k\in[1,h]}$. For $k = 1, \dots, h$, run $\mathsf{sk}_{k,kw'}^{(i)} \leftarrow \mathsf{HIBE.KeyDer}(\mathsf{MPK}', \mathsf{sk}_k^{(i)}, kw')$. Output $\mathsf{td}_{\mathsf{R},kw'} = \{\mathsf{sk}_{k,kw'}^{(i)}\}_{k\in[1,h]}$.

$\mathsf{BEKS.Test}(\mathsf{MPK}, \mathsf{ct}_{\mathsf{BEKS}}, \mathsf{td}_{\mathsf{R},kw'})$: Parse $\mathsf{MPK} = (\mathsf{MPK}', N)$, $\mathsf{ct}_{\mathsf{BEKS}} = (\mathsf{vk}, \sigma, \{\mathsf{ct}_{\mathsf{HIBE},\pi(j)}\}_{j\in[1,L]})$ and $\mathsf{td}_{\mathsf{R},kw'} = \{\mathsf{sk}_{k,kw'}\}_{k\in[1,h]}$. Output 0 if $\mathsf{OTS.Verify}(\mathsf{vk}, \sigma, \{\mathsf{ct}_{\mathsf{HIBE},\pi(j)}\}_{j\in[1,L]}) = 0$. Otherwise, for $k = 1$ to h, run $\mathsf{sk}_{k,kw',\mathsf{vk}} \leftarrow \mathsf{HIBE.KeyDer}(\mathsf{MPK}', \mathsf{sk}_{k,kw'}, \mathsf{vk})$.

```
• For $k = 1$ to $h$
    – For $j = 1$ to $L$
        ∗ Run $M \leftarrow \mathsf{HIBE.Dec}(\mathsf{MPK}', \mathsf{ct}_{\mathsf{HIBE},j},
          \mathsf{sk}_{k,kw',\mathsf{vk}})$.
        ∗ If $M = 0^\lambda$, then return 1. Otherwise,
          if $j = L$, break the loop. Otherwise,
          $j \leftarrow j + 1$.
    – If $k = h$, return 0. Otherwise, $k \leftarrow k + 1$.
```

If $i \in S$, then $\mathsf{cover} \cap \mathsf{Path}(i) \neq \emptyset$ due to the CS method. Let $x_j \in \mathsf{cover} \cap \mathsf{Path}(i)$. If $kw =$

[†] In Definition 1, a hierarchical identity is represented as a tuple of three elements in the same space $\mathsf{IDspace}$. This does not prevent the correctness of the proposed construction since (H)IBE allows us to employ any string as a public key. More precisely, if the size of keyword space $\mathsf{KWspace}$ is relatively small (e.g., $|\mathsf{KWspace}| = 2^{18}$ as mentioned in Sect. 3), then we regard $\mathsf{KWspace} \subset \mathsf{IDspace}$.

kw', then for $\mathsf{ct}_{\mathsf{HIBE}} \leftarrow \mathsf{HIBE.Enc}(\mathsf{MPK}', (x_j, kw, \mathsf{vk}), 0^\lambda)$ contained in $\mathsf{ct}_{\mathsf{BEKS}}$ and $\mathsf{sk} \leftarrow \mathsf{HIBE.KeyGen}(\mathsf{MPK}', \mathsf{MSK}, x_j)$, $\mathsf{td}_{\mathsf{R},kw} \ni \mathsf{sk}_{kw} \leftarrow \mathsf{HIBE.KeyDer}(\mathsf{MPK}', \mathsf{sk}, kw)$, and $\mathsf{sk}_{kw,\mathsf{vk}} \leftarrow \mathsf{HIBE.KeyDer}(\mathsf{MPK}', \mathsf{sk}_{kw}, \mathsf{vk})$, $0^\lambda \leftarrow \mathsf{HIBE.Dec}(\mathsf{MPK}', \mathsf{ct}_{\mathsf{HIBE}}, \mathsf{sk}_{kw,\mathsf{vk}})$ holds. Thus, correctness directly holds due to the correctness of the underlying IBE scheme and one-time signature scheme. We remark that one may require that there exists only one $\mathsf{ct}_{\mathsf{HIBE},j}$ such that $0^\lambda \leftarrow \mathsf{HIBE.Dec}(\mathsf{MPK}', \mathsf{ct}_{\mathsf{HIBE},j}, \mathsf{sk}_{k,kw',\mathsf{vk}})$ holds for some $k \in [1, h]$. For example, let a content be also encrypted and the ciphertext be preserved together with $\mathsf{ct}_{\mathsf{HIBE},j}$. The cloud server returns the j-th content ciphertext if the test algorithm finds j where $0^\lambda \leftarrow \mathsf{HIBE.Dec}(\mathsf{MPK}', \mathsf{ct}_{\mathsf{HIBE},j}, \mathsf{sk}_{k,kw',\mathsf{vk}})$ holds. If a different content is chosen according to the receiver, then finding the unique j is mandatory, and then the $\mathsf{BEKS.Trapdoor}$ algorithm outputs 0 if there exist two or more ciphertexts that the decryption results are 0^λ. Actually, the proposed construction provides the correctness in this stronger notion when the underlying HIBE scheme is weakly robust. Note that we need to introduce computational correctness in this case.

6. Security Analysis

Theorem 1. *The proposed construction is computationally consistent if* HIBE *is weakly robust.*

Proof. Let $\mathcal{A}$ be an adversary of computational consistency of the proposed construction and C be the challenger of weak robustness of HIBE. We construct an algorithm $\mathcal{B}$ that breaks weak robustness as follows. C runs $(\mathsf{MPK}', \mathsf{MSK}) \leftarrow \mathsf{HIBE.Setup}(1^\lambda)$ and sends MPK' to $\mathcal{B}$. $\mathcal{B}$ sends $\mathsf{MPK} = (\mathsf{MPK}', N)$ to $\mathcal{A}$. $\mathcal{A}$ declares (kw, kw', S^*, i^*) where either $kw \neq kw'$ or $i^* \notin S^*$. $\mathcal{B}$ runs $(\mathsf{vk}, \mathsf{sigk}) \leftarrow \mathsf{OTS.KeyGen}(1^\lambda)$, specifies $\mathsf{RSet} := \{i \mid i \in U \wedge i \notin S^*\}$ and runs $\mathsf{cover} \leftarrow \mathsf{CompSubTree}(\mathsf{BT}, \mathsf{RSet})$ where $\mathsf{cover} = \{x_1, \ldots, x_\ell\}$. Moreover, let $\mathsf{Path}(i^*) = \{x'_1, \ldots, x'_h\}$. $\mathcal{B}$ randomly chooses $x \xleftarrow{\$} \mathsf{cover}$ and $x' \xleftarrow{\$} \mathsf{Path}(i^*)$, and sets $(\mathsf{ID}_0, \mathsf{ID}'_0, \mathsf{ID}''_0) = (x, kw, \mathsf{vk})$ and $(\mathsf{ID}_1, \mathsf{ID}'_1, \mathsf{ID}''_1) = (x', kw', \mathsf{vk})$. $\mathcal{B}$ sends $(\mathsf{ID}_0, \mathsf{ID}'_0, \mathsf{ID}''_0) = (x, kw, \mathsf{vk})$, $(\mathsf{ID}_1, \mathsf{ID}'_1, \mathsf{ID}''_1) = (x', kw', \mathsf{vk})$, and $M^* = 0^\lambda$ to C.

We estimate the success probability of $\mathcal{B}$ as follows. Now, for $\mathsf{ct}_{\mathsf{BEKS}} \leftarrow \mathsf{BEKS.Enc}(\mathsf{MPK}', S^*, kw)$ and $\mathsf{td}_{\mathsf{R},kw'} \leftarrow \mathsf{BEKS.Trapdoor}(\mathsf{MPK}',\ \mathsf{sk}_{\mathsf{R}[i^*]},\ kw')$, $\mathsf{BEKS.Test}(\mathsf{MPK}',\ \mathsf{ct}_{\mathsf{BEKS}},\ \mathsf{td}_{\mathsf{R},kw'}) = 1$ holds. That is, there exist at least one $\mathsf{ct}_{\mathsf{HIBE},j}$ and $\mathsf{sk}^{(i^*)}_{k,kw',\mathsf{vk}}$ such that $0^\lambda \leftarrow \mathsf{HIBE.Dec}\ (\mathsf{MPK}', \mathsf{ct}_{\mathsf{HIBE},j}, \mathsf{sk}_{k,kw',\mathsf{vk}})$ holds. This implies that, with the probability at least $1/|\mathsf{cover}||\mathsf{Path}(i^*)| = 1/\ell h > 1/Lh$, $\mathsf{HIBE.Dec}(\mathsf{MPK}', \mathsf{ct}_{\mathsf{HIBE},j}, \mathsf{sk}_{k,kw',\mathsf{vk}}) = 0^\lambda$ holds where $\mathsf{ct}_{\mathsf{HIBE},j}$ is a ciphertext of 0^λ under the identities (x, kw, vk), $\mathsf{sk}_{k,kw',\mathsf{vk}}$ is a secret key for the identities (x', kw', vk), and $(x, kw, \mathsf{vk}) \neq (x', kw', \mathsf{vk})$. Note that if $i^* \notin S^*$, then $\mathsf{cover} \cap \mathsf{Path}(i^*) = \emptyset$. Thus, either $kw \neq kw'$ or $i^* \notin S^*$ implies $(x, kw) \neq (x', kw')$. $\mathcal{B}$ breaks weak robustness with the probability at least $1/Lh$. □

Theorem 2. *The proposed construction is outsider anonymous if* HIBE *is Anon-CPA secure and* OTS *is sEUF-CMA secure.*

Proof. Let $(kw^*_0, kw^*_1, S^*_0, S^*_1)$ be the output by the adversary $\mathcal{A}$ in the experiment. Let R^* be the number of revoked users in the challenge ciphertext, i.e., $R^* = N - |S^*_b|$ for $b = 0, 1$, and L^* be $\lfloor R^* \log(N/R^*) \rfloor$. For $b = 0, 1$, let $\mathsf{cover}_b = \{x^{(b)}_1, \ldots, x^{(b)}_{\ell_b}\}$ be determined by $\mathsf{RSet}_b := \{i \mid i \in U \wedge i \notin S^*_b\}$ and $\mathsf{cover}_b \leftarrow \mathsf{CompSubTree}(\mathsf{BT}, \mathsf{RSet}_b)$.

We define a sequence of games $\mathsf{Game}^0_0, \mathsf{Game}^0_1, \ldots, \mathsf{Game}^0_{\ell_0} = \mathsf{Game}^1_{\ell_1}, \ldots, \mathsf{Game}^1_1, \mathsf{Game}^1_0$. In Game^0_0, the challenge ciphertext is generated by S^*_0 for kw^*_0 and in Game^1_0, the challenge ciphertext is generated by S^*_1 for kw^*_1. Before giving the game descriptions, first, we construct an algorithm $\mathcal{B}_1$ that breaks sEUF-CMA security when $\mathcal{A}$ (in Game^0_0) sends a test query $(i, kw, \mathsf{ct}_{\mathsf{BEKS}})$ where $\mathsf{ct}_{\mathsf{BEKS}} = (\mathsf{vk}^*, \sigma, \{\mathsf{ct}_{\mathsf{HIBE},\pi(j)}\}_{j\in[1,L]})$, vk^* is the verification key used for generating the challenge ciphertext, and $\mathsf{OTS.Verify}(\mathsf{vk}^*, \sigma, \{\mathsf{ct}_{\mathsf{HIBE},\pi(j)}\}_{j\in[1,L]}) = 1$. The challenger of sEUF-CMA runs $(\mathsf{vk}^*, \mathsf{sigk}^*) \leftarrow \mathsf{OTS.KeyGen}(1^\lambda)$ and sends vk^* to $\mathcal{B}_1$. $\mathcal{B}_1$ generates other parameters and thus $\mathcal{B}_1$ can respond any query issued by $\mathcal{A}$. In the challenge phase, the challenge ciphertext $\mathsf{ct}^*_{\mathsf{BEKS}}$ is generated as follows. Set $\tilde{M} \xleftarrow{\$} \{0,1\}^\lambda$.

- For $j = 1, \ldots, \ell_0$: Run $\mathsf{ct}_{\mathsf{HIBE},j} \leftarrow \mathsf{HIBE.Enc}(\mathsf{MPK}', (x^{(0)}_j, kw^*_0, \mathsf{vk}^*), 0^\lambda)$.
- For $j = \ell_0 + 1, \ldots, L^*$: Run $\mathsf{ct}_{\mathsf{HIBE},j} \leftarrow \mathsf{HIBE.Enc}(\mathsf{MPK}', (\mathsf{dummy}, \mathsf{dummy}', \mathsf{vk}^*), \tilde{M})$.

$\mathcal{B}_1$ sends $\{\mathsf{ct}_{\mathsf{HIBE},\pi(j)}\}_{j\in[1,L^*]}$ to the challenger, obtains $\sigma^* \leftarrow \mathsf{OTS.Sign}(\mathsf{sigk}^*, \{\mathsf{ct}_{\mathsf{HIBE},\pi(j)}\}_{j\in[1,L^*]})$, and sets $\mathsf{ct}^*_{\mathsf{BEKS}} = (\mathsf{vk}^*, \sigma^*, \{\mathsf{ct}_{\mathsf{HIBE},\pi(j)}\}_{j\in[1,L^*]})$. Assume that $\mathcal{A}$ sends a test query $(i, kw, \mathsf{ct}_{\mathsf{BEKS}})$ such that $\mathsf{ct}_{\mathsf{BEKS}} = (\mathsf{vk}^*, \sigma', \{\mathsf{ct}'_{\mathsf{HIBE},\pi(j)}\}_{j\in[1,L]})$ and $\mathsf{OTS.Verify}(\mathsf{vk}^*, \sigma', \{\mathsf{ct}'_{\mathsf{HIBE},\pi(j)}\}_{j\in[1,L]}) = 1$. Let $\mathsf{ct}_{\mathsf{BEKS}} = \mathsf{ct}^*_{\mathsf{BEKS}}$. Then, either $i \notin S^*_0 \cup S^*_1$ or $kw \notin \{kw^*_0, kw^*_1\}$. Thus, $\mathcal{B}_1$ returns 0. Let $\mathsf{ct}_{\mathsf{BEKS}} \neq \mathsf{ct}^*_{\mathsf{BEKS}}$ and $\mathsf{vk}' = \mathsf{vk}^*$ that implies $(\sigma^*, \{\mathsf{ct}_{\mathsf{HIBE},\pi(j)}\}_{j\in[1,L^*]}) \neq (\sigma', \{\mathsf{ct}'_{\mathsf{HIBE},\pi(j)}\}_{j\in[1,L]})$. Because $\mathsf{OTS.Verify}(\mathsf{vk}^*, \sigma', \{\mathsf{ct}'_{\mathsf{HIBE},\pi(j)}\}_{j\in[1,L]}) = 1$, $\mathcal{B}_1$ outputs $(\sigma', \{\mathsf{ct}'_{\mathsf{HIBE},\pi(j)}\}_{j\in[1,L]})$ and breaks sEUF-CMA security. We remark that $\mathcal{B}_1$ fails to make a reduction for an (artificial) adversary where it works when $b = 1$ and does not work when $b = 0$. However, in this case, we can define a sequence of games in the reverse order, i.e., the challenge ciphertext is generated by S^*_1 for kw^*_1 in the first game, and is generated by S^*_0 for kw^*_0 in the last game. Thus, without loss of generality, we start Game^0_0 in our security proof.

Next, we give game descriptions of $\mathsf{Game}^0_0, \mathsf{Game}^0_1, \ldots, \mathsf{Game}^0_{\ell_0} = \mathsf{Game}^1_{\ell_1}, \ldots, \mathsf{Game}^1_1, \mathsf{Game}^1_0$ as follows. In all games, we exclude the case that $\mathcal{A}$ issues a test query containing vk^* and contained signature σ is valid under vk^*.

Game^0_t $(t = 0, 1, \ldots, \ell_0)$**:** The challenge ciphertext $\mathsf{ct}^*_{\mathsf{BEKS}}$ is generated as follows. Set $\tilde{M} \xleftarrow{\$} \{0,1\}^\lambda$. Run

$(\mathsf{vk}^*, \mathsf{sigk}^*) \leftarrow \mathsf{OTS.KeyGen}(1^\lambda)$.

- For $j = 1, \dots, \ell_0 - t$: Run $\mathsf{ct}_{\mathsf{HIBE},j} \leftarrow \mathsf{HIBE.Enc}(\mathsf{MPK}', (x_j^{(0)}, kw_0^*, \mathsf{vk}^*), 0^\lambda)$.
- For $j = \ell_0 - t + 1, \dots, L^*$: Run $\mathsf{ct}_{\mathsf{HIBE},j} \leftarrow \mathsf{HIBE.Enc}(\mathsf{MPK}', (\mathsf{dummy}, \mathsf{dummy}', \mathsf{vk}^*), \tilde{M})$.

Run $\sigma^* \leftarrow \mathsf{OTS.Sign}(\mathsf{sigk}^*, \{\mathsf{ct}_{\mathsf{HIBE},\pi(j)}\}_{j \in [1,L^*]})$ and set $\mathsf{ct}^*_{\mathsf{BEKS}} = (\mathsf{vk}^*, \sigma^*, \{\mathsf{ct}_{\mathsf{HIBE},\pi(j)}\}_{j \in [1,L^*]})$.

$\mathsf{Game}^1_{\ell_1}$**:** This is the same as $\mathsf{Game}^0_{\ell_0}$. In this game, all HIBE ciphertexts are $\mathsf{ct}_{\mathsf{HIBE},j} \leftarrow \mathsf{HIBE.Enc}(\mathsf{MPK}', (\mathsf{dummy}, \mathsf{dummy}', \mathsf{vk}^*), \tilde{M})$ for all $j = 1, 2, \dots, L^*$.

$\mathsf{Game}^1_{t'}$ $(t' = \ell_1 - 1, \dots, 1, 0)$**:** The challenge ciphertext $\mathsf{ct}^*_{\mathsf{BEKS}}$ is generated as follows. Set $\tilde{M} \xleftarrow{\$} \{0,1\}^\lambda$. Run $(\mathsf{vk}^*, \mathsf{sigk}^*) \leftarrow \mathsf{OTS.KeyGen}(1^\lambda)$.

- For $j = 1, \dots, \ell_1 - t'$: Run $\mathsf{ct}_{\mathsf{HIBE},j} \leftarrow \mathsf{HIBE.Enc}(\mathsf{MPK}', (x_j^{(1)}, kw_1^*, \mathsf{vk}^*), 0^\lambda)$.
- For $j = \ell_1 + t' + 1, \dots, L^*$: Run $\mathsf{ct}_{\mathsf{HIBE},j} \leftarrow \mathsf{HIBE.Enc}(\mathsf{MPK}', (\mathsf{dummy}, \mathsf{dummy}', \mathsf{vk}^*), \tilde{M})$.

Run $\sigma^* \leftarrow \mathsf{OTS.Sign}(\mathsf{sigk}^*, \{\mathsf{ct}_{\mathsf{HIBE},\pi(j)}\}_{j \in [1,L^*]})$ and set $\mathsf{ct}^*_{\mathsf{BEKS}} = (\mathsf{vk}^*, \sigma^*, \{\mathsf{ct}_{\mathsf{HIBE},\pi(j)}\}_{j \in [1,L^*]})$.

Let $\mathsf{Adv}^{0,t}_{\mathsf{BEKS},\mathcal{A}}(\lambda, N)$ and $\mathsf{Adv}^{1,t'}_{\mathsf{BEKS},\mathcal{A}}(\lambda, N)$ be $\mathcal{A}$'s advantage of winning in Game^0_t and $\mathsf{Game}^1_{t'}$, respectively. By definition, $\mathsf{Adv}^{\mathsf{outsider\text{-}anon}}_{\mathsf{BEKS},\mathcal{A}}(\lambda, N) = |\mathsf{Adv}^{0,0}_{\mathsf{BEKS},\mathcal{A}}(\lambda, N) - \mathsf{Adv}^{1,0}_{\mathsf{BEKS},\mathcal{A}}(\lambda, N)|$. We show that there exists a series of algorithms $\mathcal{B}'_t$ and $\mathcal{B}'_{t'}$ where $|\mathsf{Adv}^{0,0}_{\mathsf{BEKS},\mathcal{A}}(\lambda, N) - \mathsf{Adv}^{1,0}_{\mathsf{BEKS},\mathcal{A}}(\lambda, N)| \leq \sum_{t=1}^{L^*} \mathsf{Adv}^{\mathsf{Anon\text{-}CPA}}_{\mathsf{HIBE},\mathcal{B}'_t}(\lambda) + \sum_{t'=1}^{L^*} \mathsf{Adv}^{\mathsf{Anon\text{-}CPA}}_{\mathsf{HIBE},\mathcal{B}'_{t'}}(\lambda)$ as follows.

Lemma 1. *For* $t = 1, \dots, \ell_0$, *there exists an algorithm* $\mathcal{B}'_t$ *where* $|\mathsf{Adv}^{0,t-1}_{\mathsf{BEKS},\mathcal{A}}(\lambda, N) - \mathsf{Adv}^{0,t}_{\mathsf{BEKS},\mathcal{A}}(\lambda, N)| \leq \mathsf{Adv}^{\mathsf{Anon\text{-}CPA}}_{\mathsf{HIBE},\mathcal{B}'_t}(\lambda)$ *holds.*

Proof. We construct an algorithm $\mathcal{B}'_t$ that breaks Anon-CPA security as follows. Let C be the challenger of Anon-CPA. C runs $(\mathsf{MPK}', \mathsf{MSK}) \leftarrow \mathsf{HIBE.Setup}(1^\lambda)$ and sends MPK' to $\mathcal{B}'_t$. $\mathcal{B}'_t$ sends $\mathsf{MPK} = (\mathsf{MPK}', N)$ to $\mathcal{A}$. $\mathcal{B}'_t$ runs $(\mathsf{vk}^*, \mathsf{sigk}^*) \leftarrow \mathsf{OTS.KeyGen}(1^\lambda)$.

- When $\mathcal{A}$ issues a trapdoor query (i, kw), $\mathcal{B}'_t$ sets $\mathsf{Path}(i) = \{x'_1, \dots, x'_h\}$. For $j = 1, \dots, h$, $\mathcal{B}'_t$ sends (x'_j, kw) to C as a key extraction query. C runs $\mathsf{sk}_j \leftarrow \mathsf{HIBE.KeyGen}(\mathsf{MSK}, x'_j)$ and $\mathsf{sk}^{(i)}_{j,kw} \leftarrow \mathsf{HIBE.KeyDer}(\mathsf{MPK}', \mathsf{sk}_j, kw)$, and sends $\mathsf{sk}^{(i)}_{j,kw}$ to $\mathcal{B}'_t$. $\mathcal{B}'_t$ returns $\mathsf{td}_{\mathsf{R},kw} = \{\mathsf{sk}^{(i)}_{j,kw}\}_{j \in [1,h]}$ to $\mathcal{A}$.

- When $\mathcal{A}$ issues a corruption query i, $\mathcal{B}'_t$ sets $\mathsf{Path}(i) = \{x'_1, \dots, x'_h\}$. For $j = 1, \dots, h$, $\mathcal{B}'_t$ sends x'_j to C as a key extraction query. C runs $\mathsf{sk}_j \leftarrow \mathsf{HIBE.KeyGen}(\mathsf{MSK}, x'_j)$ and sends sk_j to $\mathcal{B}'_t$. $\mathcal{B}$ returns $\mathsf{sk}_{\mathsf{R}[j]} = \{\mathsf{sk}^{(j)}_k\}_{k \in [1,h]}$ to $\mathcal{A}$.

- When $\mathcal{A}$ issues a test query $(i, kw, \mathsf{ct}_{\mathsf{BEKS}})$ such that $\mathsf{ct}_{\mathsf{BEKS}} = (\mathsf{vk}, \sigma, \{\mathsf{ct}_{\mathsf{HIBE},\pi(j)}\}_{j \in [1,L]})$ and $\mathsf{vk} \neq \mathsf{vk}^*$, $\mathcal{B}'_t$ returns 0 if $\mathsf{OTS.Verify}(\mathsf{vk}, \sigma, \{\mathsf{ct}_{\mathsf{HIBE},\pi(j)}\}_{j \in [1,L]}) = 0$. Otherwise, $\mathcal{B}'_t$ sets $\mathsf{Path}(i) = \{x'_1, \dots, x'_h\}$, and for $k = 1, \dots, h$, $\mathcal{B}'_t$ sends (x'_k, kw, vk) to C as a key extraction query. C runs $\mathsf{sk}_k \leftarrow \mathsf{HIBE.KeyGen}(\mathsf{MSK}, x'_k)$, $\mathsf{sk}^{(i)}_{k,kw} \leftarrow \mathsf{HIBE.KeyDer}(\mathsf{MPK}', \mathsf{sk}_k, kw)$, and $\mathsf{sk}^{(i)}_{k,kw,\mathsf{vk}} \leftarrow \mathsf{HIBE.KeyDer}(\mathsf{MPK}', \mathsf{sk}_{k,kw}, \mathsf{vk})$, and sends $\mathsf{sk}^{(i)}_{k,kw,\mathsf{vk}}$ to $\mathcal{B}'_t$. $\mathcal{B}'_t$ responds the test query as follows.
  - For $k = 1$ to h
    - ∗ For $j = 1$ to L
      - · Run $M \leftarrow \mathsf{HIBE.Dec}(\mathsf{MPK}', \mathsf{ct}_{\mathsf{HIBE},j}, \mathsf{sk}_{k,kw,\mathsf{vk}})$.
      - · If $M = 0^\lambda$, then return 1. Otherwise, if $j = L$, break the loop. Otherwise, $j \leftarrow j + 1$.
    - ∗ If $k = h$, return 0. Otherwise, $k \leftarrow k + 1$.

In the challenge phase, $\mathcal{A}$ declares $(kw_0^*, kw_1^*, S_0^*, S_1^*)$. $\mathcal{B}$ specifies $\mathsf{RSet}_0 := \{i \mid i \in U \wedge i \notin S_0^*\}$ and $\mathsf{cover}_0 \leftarrow \mathsf{CompSubTree}(\mathsf{BT}, \mathsf{RSet}_0)$. Let $\mathsf{cover}_0 = \{x_1^{(0)}, \dots, x_{\ell_0}^{(0)}\}$. Here, $\mathcal{B}'_t$ did not send a key extraction query for all $x \in \mathsf{cover}_0$ directly because $V \cap (S_0^* \cup S_1^*) = \emptyset$. More precisely, if $\mathcal{B}'_t$ issued a key extraction query for $x \in \mathsf{cover}_0$, then $\mathcal{B}'_t$ sends either (1) (x, kw) where $kw \notin \{kw_0^*, kw_1^*\}$ or (2) (x, kw, vk) where $\mathsf{vk} \neq \mathsf{vk}^*$. Thus, we can set $(\mathsf{ID}_0, \mathsf{ID}'_0, \mathsf{ID}''_0) = (x_j^{(0)}, kw_0^*, \mathsf{vk}^*)$ below. $\mathcal{B}'_t$ generates the challenge ciphertext $\mathsf{ct}^*_{\mathsf{BEKS}}$ as follows. Set $\tilde{M} \xleftarrow{\$} \{0,1\}^\lambda$.

- For $j = 1, \dots, \ell_0 - t$: Run $\mathsf{ct}_{\mathsf{HIBE},j} \leftarrow \mathsf{HIBE.Enc}(\mathsf{MPK}', (x_j^{(0)}, kw_0^*, \mathsf{vk}^*), 0^\lambda)$.
- For $j = \ell_0 - t + 1$, $\mathcal{B}'_t$ sets $(\mathsf{ID}_0, \mathsf{ID}'_0, \mathsf{ID}''_0) = (x_j^{(0)}, kw_0^*, \mathsf{vk}^*)$, $(\mathsf{ID}_1, \mathsf{ID}'_1, \mathsf{ID}''_1) = (\mathsf{dummy}, \mathsf{dummy}', \mathsf{vk}^*)$, $M_0^* = 0^\lambda$, and $M_1^* = \tilde{M}$, and sends $((\mathsf{ID}_0, \mathsf{ID}'_0, \mathsf{ID}''_0), (\mathsf{ID}_1, \mathsf{ID}'_1, \mathsf{ID}''_1), M_0^*, M_1^*)$ to C as the challenge query. C generates $\mathsf{ct}^*_{\mathsf{HIBE}} \leftarrow \mathsf{HIBE.Enc}(\mathsf{MPK}', (\mathsf{ID}_b, \mathsf{ID}'_b, \mathsf{vk}^*), M_b^*)$ and sends $\mathsf{ct}^*_{\mathsf{HIBE}}$ to $\mathcal{B}'_t$. $\mathcal{B}'_t$ sets $\mathsf{ct}_{\mathsf{HIBE},j} = \mathsf{ct}^*_{\mathsf{HIBE}}$.
- For $j = \ell_0 - t + 2, \dots, L^*$: Run $\mathsf{ct}_{\mathsf{HIBE},j} \leftarrow \mathsf{HIBE.Enc}(\mathsf{MPK}', (\mathsf{dummy}, \mathsf{dummy}', \mathsf{vk}^*), \tilde{M})$.

$\mathcal{B}'_t$ runs $\sigma^* \leftarrow \mathsf{OTS.Sign}(\mathsf{sigk}^*, \{\mathsf{ct}_{\mathsf{HIBE},\pi(j)}\}_{j \in [1,L^*]})$ and sets $\mathsf{ct}^*_{\mathsf{BEKS}} = (\mathsf{vk}^*, \sigma^*, \{\mathsf{ct}_{\mathsf{HIBE},\pi(j)}\}_{j \in [1,L^*]})$. $\mathcal{B}'_t$ sends $\mathsf{ct}^*_{\mathsf{BEKS}} = (\mathsf{vk}^*, \sigma^*, \{\mathsf{ct}_{\mathsf{HIBE},\pi(j)}\}_{j \in [1,L^*]})$ to $\mathcal{A}$.

- When $\mathcal{A}$ issues a trapdoor query (i, kw), $\mathcal{B}'_t$ returns $\perp$ if $i \in S_0^* \cup S_1^*$ and $kw \in \{kw_0^*, kw_1^*\}$. Otherwise, $\mathcal{B}'_t$ proceeds as in the pre-challenge phase.

- When $\mathcal{A}$ issues a corruption query i, $\mathcal{B}'_t$ returns $\perp$ if $i \in S_0^* \cup S_1^*$. Otherwise, $\mathcal{B}$ proceeds as in the pre-challenge phase.

- When $\mathcal{A}$ issues a test query $(i, kw, \mathsf{ct}_{\mathsf{BEKS}})$ such that $\mathsf{ct}_{\mathsf{BEKS}} = (\mathsf{vk}, \sigma, \{\mathsf{ct}'_{\mathsf{HIBE},\pi(j)}\}_{j \in [1,L]})$, $\mathcal{B}'_t$ returns $\perp$ if $i \in S_0^* \cup S_1^*$ and $\mathsf{ct}_{\mathsf{BEKS}} = \mathsf{ct}^*_{\mathsf{BEKS}}$. Otherwise, $\mathcal{B}$ proceeds as in the pre-challenge phase.

Finally, $\mathcal{A}$ outputs b'. $\mathcal{B}'_t$ outputs b'. If $b = 0$, then $\mathcal{B}'_t$ simulates Game^0_{t-1} and if $b = 1$, then $\mathcal{B}'_t$ simulates Game^0_t. Thus, the claim holds. □

The proof of Lemma 2 is almost the same as that of Lemma 1, except that $\mathcal{B}'_{t'}$ specifies $\mathsf{RSet}_1 := \{i \mid i \in U \wedge i \notin S^*_1\}$ and $\mathsf{cover}_1 \leftarrow \mathsf{CompSubTree}(\mathsf{BT}, \mathsf{RSet}_1)$ in the challenge phase. Thus, we omit the proof.

Lemma 2. *For $t' = \ell_1 - 1, \ldots, 0$, there exists an algorithm $\mathcal{B}'_{t'}$ where $|\mathsf{Adv}^{1,t'+1}_{\mathsf{BEKS},\mathcal{A}}(\lambda, N) - \mathsf{Adv}^{1,t'}_{\mathsf{BEKS},\mathcal{A}}(\lambda, N)| \leq \mathsf{Adv}^{\mathsf{Anon\text{-}CPA}}_{\mathsf{HIBE},\mathcal{B}'_{t'}}(\lambda)$ holds.*

By Lemma 1 and Lemma 2, we conclude the proof of Theorem 2. □

7. Conclusion

In this paper, from 3-level anonymous and weakly robust HIBE we proposed a generic construction of outsider anonymous BEKS with sublinear size ciphertexts. Our result could be regarded as a stepping stone to propose an outsider anonymous BAEKS scheme with sublinear-size ciphertexts. Since we employed the CS method, the subset difference (SD) method could be employed by adding more hierarchy level, due to the SD method in the public key setting from HIBE [53]. We leave them as open problems. Also, it would be interesting to investigate whether other efficient outsider anonymous schemes, e.g. [54], [55], can be employed in the BEKS/BAEKS context or not.

The proposed construction requires approximately $L/2$-times HIBE decryption procedures where $L = \lfloor R \log(N/R) \rfloor$. To reduce the number of decryption attempts in the generic construction of anonymous broadcast encryption, Libert et al. [14] proposed an anonymous hint system that provides $O(1)$ decryption cost in terms of the number of cryptographic operations. Moreover, Fazio and Perera [15] also considered to reduce the number of decryption procedure by employing trapdoor test of twin Diffie-Hellman problem [56]. In both attempts, additional secret values are introduced in addition to the decryption key. That is, as mentioned in [28], if these systems are employed in BEKS, then the cloud server, that runs the $\mathsf{BEKS.Test}$ algorithm, obtains information about the receivers before running the test algorithm. Consequently, we did not employ these systems in this paper. We leave this task as an interesting future work.

Acknowledgments

The main part of this study was done when the first author, Keita Emura, was with the National Institute of Information and Communications Technology, Japan. This work was supported by JSPS KAKENHI Grant Number JP21K11897.

References

[1] D. Boneh, G.D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," EUROCRYPT, pp.506–522, 2004.

[2] N. Attrapadung, J. Furukawa, and H. Imai, "Forward-secure and searchable broadcast encryption with short ciphertexts and private keys," ASIACRYPT, pp.161–177, 2006.

[3] S. Chatterjee and S. Mukherjee, "Keyword search meets membership testing: Adaptive security from SXDH," INDOCRYPT, pp.21–43, 2018.

[4] M. Ambrona, G. Barthe, and B. Schmidt, "Generic transformations of predicate encodings: Constructions and applications," CRYPTO, pp.36–66, 2017.

[5] J. Chen, R. Gay, and H. Wee, "Improved dual system ABE in prime-order groups via predicate encodings," EUROCRYPT, pp.595–624, 2015.

[6] J. Chen and J. Gong, "ABE with tag made easy — Concise framework and new instantiations in prime-order groups," ASIACRYPT, pp.35–65, 2017.

[7] P. Jiang, F. Guo, and Y. Mu, "Efficient identity-based broadcast encryption with keyword search against insider attacks for database systems," Theoretical Computer Science, vol.767, pp.51–72, 2019.

[8] A. Kiayias, O. Oksuz, A. Russell, Q. Tang, and B. Wang, "Efficient encrypted keyword search for multi-user data sharing," ESORICS, pp.173–195, 2016.

[9] M. Ma, S. Fan, and D. Feng, "Multi-user certificateless public key encryption with conjunctive keyword search for cloud-based telemedicine," Journal of Information Security and Applications, vol.55, p.102652, 2020.

[10] T. Feng and J. Si, "Certificateless searchable encryption scheme in multi-user environment," Cryptography, vol.6, no.4, p.61, 2022.

[11] K. Zhang, M. Wen, R. Lu, and K. Chen, "Multi-client sub-linear boolean keyword searching for encrypted cloud storage with owner-enforced authorization," IEEE Trans. Dependable Secure Comput., vol.18, no.6, pp.2875–2887, 2021.

[12] N. Yang, Q. Zhou, Q. Huang, and C. Tang, "Multi-recipient encryption with keyword search without pairing for cloud storage," J. Cloud Comp., vol.11, p.10, 2022.

[13] M. Ali, H. Ali, T. Zhong, F. Li, Z. Qin, and A.A. Ahmed Abdelrahaman, "Broadcast searchable keyword encryption," IEEE CSE, pp.1010–1016, 2014.

[14] B. Libert, K.G. Paterson, and E.A. Quaglia, "Anonymous broadcast encryption: Adaptive security and efficient constructions in the standard model," Public Key Cryptography, pp.206–224, 2012.

[15] N. Fazio and I.M. Perera, "Outsider-anonymous broadcast encryption with sublinear ciphertexts," Public Key Cryptography, pp.225–242, 2012.

[16] A. Barth, D. Boneh, and B. Waters, "Privacy in encrypted content distribution using private broadcast encryption," Financial Cryptography and Data Security, pp.52–64, 2006.

[17] H. Kobayashi, Y. Watanabe, K. Minematsu, and J. Shikata, "Tight lower bounds and optimal constructions of anonymous broadcast encryption and authentication," Des. Codes Cryptogr., vol.91, no.7, pp.2523–2562, 2023.

[18] A. Kiayias and K. Samari, "Lower bounds for private broadcast encryption," Information Hiding, pp.176–190, 2012.

[19] J. Li and J. Gong, "Improved anonymous broadcast encryptions — Tight security and shorter ciphertext," ACNS, pp.497–515, 2018.

[20] X. Liu, K. He, G. Yang, W. Susilo, J. Tonien, and Q. Huang, "Broadcast authenticated encryption with keyword search," ACISP, pp.193–213, 2021.

[21] B. Qin, H. Cui, X. Zheng, and D. Zheng, "Improved security model for public-key authenticated encryption with keyword search," ProvSec, pp.19–38, 2021.

[22] L. Cheng and F. Meng, "Public key authenticated encryption with keyword search from LWE," ESORICS, pp.303–324, 2022.

[23] K. Emura, "Generic construction of public-key authenticated encryption with keyword search revisited: Stronger security and efficient construction," ACM APKC, pp.39–49, 2022.

[24] Q. Huang and H. Li, "An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks," Information Sciences, vols.403–404, pp.1–14, 2017.
[25] Z. Liu, Y. Tseng, R. Tso, M. Mambo, and Y. Chen, "Public-key authenticated encryption with keyword search: Cryptanalysis, enhanced security, and quantum-resistant instantiation," ACM ASIACCS, pp.423–436, 2022.
[26] L. Yao, J. Weng, A. Yang, X. Liang, Z. Wu, Z. Jiang, and L. Hou, "Scalable CCA-secure public-key authenticated encryption with keyword search from ideal lattices in cloud computing," Information Sciences, vol.624, pp.777–795, 2023.
[27] S. Mukherjee, "Statistically consistent broadcast authenticated encryption with keyword search: Adaptive security from standard assumptions," ACISP, pp.523–552, 2023.
[28] K. Emura, "Generic construction of fully anonymous broadcast authenticated encryption with keyword search with adaptive corruptions," IET Information Security, vol.2023, pp.9922828:1–9922828:12, 2023.
[29] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," CRYPTO, pp.41–62, 2001.
[30] R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext security from identity-based encryption," EUROCRYPT, pp.207–222, 2004.
[31] M. Abdalla, M. Bellare, and G. Neven, "Robust encryption," J. Cryptol., vol.31, no.2, pp.307–350, 2018.
[32] M. Abdalla, M. Bellare, and G. Neven, "Robust encryption," TCC, pp.480–497, 2010.
[33] S.C. Ramanna and P. Sarkar, "Efficient (anonymous) compact HIBE from standard assumptions," ProvSec, pp.243–258, 2014.
[34] R. Langrehr and J. Pan, "Hierarchical identity-based encryption with tight multi-challenge security," Public-Key Cryptography, pp.153–183, 2020.
[35] O. Blazy, E. Kiltz, and J. Pan, "(Hierarchical) Identity-based encryption from affine message authentication," CRYPTO, pp.408–425, 2014.
[36] S. Agrawal, D. Boneh, and X. Boyen, "Efficient lattice (H)IBE in the standard model," EUROCRYPT, pp.553–572, 2010.
[37] D. Boneh and X. Boyen, "Efficient selective-ID secure identity-based encryption without random oracles," EUROCRYPT, pp.223–238, 2004.
[38] S. Yamada, "Asymptotically compact adaptively secure lattice IBEs and verifiable random functions via generalized partitioning techniques," CRYPTO, pp.161–193, 2017.
[39] K. Asano, K. Emura, and A. Takayasu, "More efficient adaptively secure lattice-based IBE with equality test in the standard model," ISC, pp.75–83, 2022.
[40] T. Jager, R. Kurek, and D. Niehues, "Efficient adaptively-secure IB-KEMs and VRFs via near-collision resistance," Public-Key Cryptography, pp.596–626, 2021.
[41] S.C. Ramanna and P. Sarkar, "Anonymous constant-size ciphertext HIBE from asymmetric pairings," IMACC, pp.344–363, 2013.
[42] K. Lee, J.H. Park, and D.H. Lee, "Anonymous HIBE with short ciphertexts: Full security in prime order groups," Des. Codes Cryptogr., vol.74, no.2, pp.395–425, 2015.
[43] S. Agrawal, D. Boneh, and X. Boyen, "Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE," CRYPTO, pp.98–115, 2010.
[44] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," J. Cryptol., vol.25, no.4, pp.601–639, 2012.
[45] X. Boyen and Q. Li, "Towards tightly secure lattice short signature and ID-based encryption," ASIACRYPT, pp.404–434, 2016.
[46] D. Boneh and X. Boyen, "Efficient selective-ID secure identity based encryption without random oracles," IACR Cryptology ePrint Archive, p.172, 2004. https://eprint.iacr.org/2004/172
[47] T. Yamakawa and M. Zhandry, "Classical vs quantum random oracles," EUROCRYPT, pp.568–597, 2021.
[48] M. Zhandry, "Secure identity-based encryption in the quantum random oracle model," CRYPTO, pp.758–775, 2012.
[49] K. Singh, C.P. Rangan, and A.K. Banerjee, "Adaptively secure efficient lattice (H)IBE in standard model with short public parameters," SPACE, pp.153–172, 2012.
[50] W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation (extended abstract)," CRYPTO, pp.137–152, 1998.
[51] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," ACM CCS, pp.417–426, ACM, 2008.
[52] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions," J. Cryptol., vol.21, no.3, pp.350–391, 2008.
[53] Y. Dodis and N. Fazio, "Public key broadcast encryption for stateless receivers," ACM DRM, pp.61–80, 2002.
[54] M. Mandal and R. Dutta, "Efficient identity-based outsider anonymous public-key trace and revoke with constant ciphertext-size and fast decryption," Inscrypt, pp.365–380, 2019.
[55] M. Mandal and K. Nuida, "Identity-based outsider anonymous broadcast encryption with simultaneous individual messaging," Network and System Security, pp.167–186, 2020.
[56] D. Cash, E. Kiltz, and V. Shoup, "The twin Diffie-Hellman problem and applications," EUROCRYPT, pp.127–145, 2008.

Keita Emura received M.E. degrees from Kanazawa University in 2004. He was with Fujitsu Hokuriku Systems Ltd., from 2004 to 2006. He received the Ph.D. degree in information science from the Japan Advanced Institute of Science and Technology (JAIST) in 2010, where he was with the Center for Highly Dependable Embedded Systems Technology as a Post-Doctoral Researcher in 2010–2012. From 2012 to 2023, he worked at the National Institute of Information and Communications Technology (NICT). He has been an Associate Professor at Kanazawa University since 2023. His research interests include public-key cryptography and information security. He was a recipient of the SCIS Innovation Paper Award from IEICE in 2012, the CSS Best Paper Award from IPSJ in 2016, the IPSJ Yamashita SIG Research Award in 2017, and the Best Paper Award from ProvSec 2022. He is a member of IEICE, IPSJ, and IACR.

Kaisei Kajita received the B.S. degree from University of Electro Communication in 2015 and M.S. degree from Tokyo Institute of Technology in 2017. He joined NHK (Japan Broadcasting Corporation) in 2017. He is currently a research engineer of NHK Science & Technology Research Laboratories. His research interest include cryptography, information security, Integrated Broadcast-Broadband system.

Go Ohtake received the B.E. and M.E. degrees from Tokyo Institute of Technology, Tokyo, Japan in 1999 and 2001, respectively. He joined NHK (Japan Broadcasting Corporation) in 2001 and received Ph.D. degree from Institute of Information Security in 2009. He was a visiting researcher at University of Calgary from December 2014 to November 2015. He is currently a chief of Internet Service Systems Research Division, NHK Science and Technology Research Laboratories. His research interests include public key cryptography and its application for copyright protection and privacy preserving.