Designs, Codes and Cryptography (2023) 91:2523–2562
https://doi.org/10.1007/s10623-023-01211-x

Tight lower bounds and optimal constructions of anonymous broadcast encryption and authentication

Hirokazu Kobayashi[1] · **Yohei Watanabe**[2] · **Kazuhiko Minematsu**[1,3] · **Junji Shikata**[1]

Received: 31 March 2022 / Revised: 2 January 2023 / Accepted: 11 March 2023 /
Published online: 3 April 2023

Abstract
Broadcast Encryption (BE) is public-key encryption allowing a sender to encrypt a message by specifing recipients, and only the specified recipients can decrypt the message. In several BE applications, since the privacy of recipients allowed to access the message is often as important as the confidentiality of the message, anonymity is introduced as an additional but important security requirement for BE. Kiayias and Samari (IH 2013) presented an asymptotic lower bound on the ciphertext sizes in BE schemes satisfying anonymity (ANO-BE for short). More precisely, their lower bound is derived under the assumption that ANO-BE schemes have a special property. However, it is insufficient to show their lower bound is asymptotically tight since it is unclear whether existing ANO-BE schemes meet the special property. In this work, we derive asymptotically tight lower bounds on the ciphertext size in ANO-BE by assuming only properties that most existing ANO-BE schemes satisfy. With a similar technique, we first derive asymptotically tight lower bounds on the authenticator sizes in Anonymous Broadcast Authentication (ABA). Furthermore, we extend the above result and present (non-asymptotically) tight lower and upper bounds on the ciphertext sizes in ANO-BE. We show that a variant of ANO-BE scheme proposed by Li and Gong (ACNS 2018) is optimal. We also provide tight bounds on the authenticator sizes in ABA via the same approach as ANO-BE, and propose an optimal construction for ABA.

Communicated by M. Paterson.

✉ Hirokazu Kobayashi
kobayashi.hirokazu.4105@gmail.com

Yohei Watanabe
watanabe@uec.ac.jp

Kazuhiko Minematsu
minematsu-kazuhiko-bk@ynu.ac.jp

Junji Shikata
shikata-junji-rb@ynu.ac.jp

[1] Yokohama National University, 79-7 Tokiwadai, Hodogaya-ku, Yokohama, Kanagawa 240-8501, Japan

[2] The University of Electro-Communications, 1-5-1 Chofugaoka, Chofu, Tokyo 182-8585, Japan

[3] NEC Corporation, 1753 Shimonumabe, Kawasaki, Kanagawa 211-8666, Japan

Keywords Broadcast encryption · Broadcast authentication · Anonymity · Lower bound

Mathematics Subject Classification 11T71 · 94A60

1 Introduction

(Anonymous) Broadcast encryption *Broadcast Encryption* (BE) [11] enables a sender to encrypt a message by designating a set of recipients so that only designated recipients can decrypt the encrypted message. In more detail, in a BE system, the sender encrypts a message m to a subset $\mathcal{S}$, called a *privileged set*, chosen from N recipients. Any recipient in the privileged set $\mathcal{S}$ can decrypt the corresponding ciphertexts $\mathsf{ct}_{\mathcal{S}}$, but the recipients outside of $\mathcal{S}$ cannot. BE has several applications such as pay-TV services and access control in encrypted file systems thanks to its functionality. The scheme is said to be *collusion resistant*, which is a de-facto standard security notion of BE, even if all of recipients outside of $\mathcal{S}$ collude they cannot obtain any information about an encrypted message. To date, many collusion-resistant BE schemes have been proposed (e.g., [1, 2, 5, 6, 15, 16, 38, 40]).

These schemes guarantee the confidentiality of the message, but the information of the privileged set is transmitted with the ciphertext publicly for decryption in the schemes while the confidentiality of the recipients authorized to access the message is an important security requirement from a practical perspective. For example, the pay-TV service sometimes requires users' privacy as well as the confidentiality of contents. To address to the security requirement, several works [3, 20, 24, 25] have proposed BE schemes meeting *anonymity*,[1] which ensures that no information on the designated recipients in $\mathcal{S}$ is leaked from ciphertexts $\mathsf{ct}_{\mathcal{S}}$. Two main notions were introduced for anonymity, called *anonymity* and *full anonymity* by Barth et al. [3] and Kiayias and Samari [20], respectively. Anonymity guarantees that no information on a set of designated recipients is leaked from ciphertexts except for its size while full anonymity guarantees that ciphertexts never leak even the information on the size of the set. Also Fazio et al. [10] introduced a weaker notion of anonymity, called *outsider anonymity*, where recipients in a privileged set are not considered to be malicious. Previous work in [10, 27] has presented Anonymous BE schemes with compact ciphertexts using this notion.[2] But the notion may not be sufficient for the security requirement of some BE applications since an adversary in a privileged set can obtain information on other designated recipients. Throught this paper, we do not deal with outsider anonymity, and refer to BE with anonymity and full anonymity as ANO-BE and Full-ANO-BE, respectively. Also, we refer to ANO-BE and Full-ANO-BE collectively as *Anonymous BE*.

There is a MAC variant of Anonymous BE, *Anonymous Broadcast Authentication* (ABA) [37]. ABA enables a sender to choose an *arbitrary subset* of receivers so that only the designated receivers can check the validity of a pair of a message and its authenticator. Moreover, ABA achieves anonymity; the authenticator does not reveal any information on which receivers are designated.[3] ABA is expected to be a core cryptographic primitive for a remote-control system over IoT networks [37]. In such a system based on ABA, a systems manager can choose an arbitrary command to have only the designated IoT devices exe-

[1] The term *privacy* is often used instead of anonymity (e.g., [3, 20]).

[2] Precisely, Mandal and Nuida [27] proposed an "identity-based outsider anonymous broadcast encryption scheme with personalized messages" with constant-size ciphertexts, which is a variant of BE with outsider anonymity. See [27] for more details.

[3] Note that ABA has different functionality from ring signatures [35]; ABA provides anonymity of receivers, while ring signatures guarantees anonymity of senders.

cute it. For example, the systems manager can bring IoT devices infected with malware to a halt remotely and securely. Moreover, anonymity of ABA guarantees that authenticators do not reveal any information on which devices are designated, which is sensitive information (see [37] for details). In this work, we also give an analysis of the authenticator sizes required for ABA, though we mainly focus on Anonymous BE.

Ciphertext size of anonymous BE The previous work [3, 20, 24, 25] has presented several Anonymous BE schemes having ciphertexts where its size grows linearly with the number of designated recipients or all recipients. Specifically, the ciphertext sizes of the ANO-BE schemes are $O(|\mathcal{S}| \cdot \kappa)$ and those of the Full-ANO-BE schemes are $O(N \cdot \kappa)$, where $|\mathcal{S}|$ and N are the numbers of designated recipients and all recipients in the system, respectively, and κ is a security parameter. Therefore, these constructions establish upper bounds on the ciphertext-sizes of Anonymous BEs.

On the other hand, Kiayias and Samari [20] investigated lower bounds on ciphertext-sizes of Anonymous BEs (i.e., ANO-BE and Full-ANO-BE). In particular, they showed that the ciphertext-sizes are required $\Omega(|\mathcal{S}| \cdot \kappa)$ for ANO-BE and $\Omega(N \cdot \kappa)$ for Full-ANO-BE, for *a limited class* of (Anonymous) BE and listed several BE schemes in [3, 25, 30] in the class.[4]

Previous work and its issue We emphasize that Kiayias and Samari implicitly assumed a special property for BE schemes in their main theorem [20, Theorem 1]. More precisely, they indeed proved "if a BE scheme is anonymous and has the special property, then the lower bound holds." However, it is hard to check whether the existing Anonymous BEs in the limited class (e.g., [3, 20, 25]) meet the property (see Sect. 1.2 for details), and it is not clearly shown that their lower bound on the ciphertext-sizes is asymptotically tight.

1.1 Our contributions

Asymptotically tight lower bounds In this paper, assuming only properties most existing (Anonymous) BE schemes have, we show that asymptotic lower bounds on ciphertext size for ANO-BE and Full-ANO-BE are $\Omega(|\mathcal{S}| \cdot \kappa)$ and $\Omega(N \cdot \kappa)$, respectively. We note that our lower bounds are asymptotically tight since they are applicable to the existing Anonymous BE schemes while Kiayias and Samari's ones are not. Our results also show that it is impossible to modify existing non-Anonymous BE schemes to meet anonymity unless their ciphertext size meets our lower bound, since the properties we assume can be applied for existing (even non-Anonymous) BE schemes.

We derive the lower bounds by extending the Kiayias and Samari's approach [20]: they considered Atomic BE (AtBE) allowing each ciphertext and decryption key to be explicitly divided into multiple sub-elements, called *atomic ciphertexts* and *decryption keys*, respectively, and the AtBE covers several BE schemes in [3, 25, 30]. They then showed lower bounds on the number of atomic ciphertexts in anonymous AtBE schemes instead of deriving lower bounds on the ciphertext-sizes directly. However, in the proof, they implicitly assumed a special property for AtBE schemes, which is hard to be applied to the existing schemes.

To provide the lower bounds without the special property, we modify the Kiayias and Samari's strategy as follows: first, we extract several properties of existing BE schemes to derive a lower bound without the special property. Also, to formalize these properties, we modify the Kiayias and Samari's AtBE, which was given only an informal syntax in [20]. Note that our AtBE covers a broad range of (both Anonymous and non-Anonymous) BE

[4] Kiayias and Samari also derived lower bounds on the ciphertext sizes $\Omega(N + \kappa)$ required for *any* Full-ANO-BE [20, Lemma 2]. However, it is unclear whether the lower bound is asymptotically tight, because no Full-ANO-BE constructions attain it.

schemes [1–3, 6, 15, 16, 24, 25, 30, 38]. We then provide lower bounds on the number of atomic ciphertexts in our AtBE with anonymity.

We summarize the differences between Kiayias and Samari's analysis and ours below.

- We assume several properties that most of the existing BE schemes have. To formally describe them, we give a formal syntax of AtBE, whereas Kiayias and Samari considered an informal one.
- Our lower bounds hold for most of the previous Anonymous BEs (i.e., BE schemes in [3, 24, 25]), since we only assume the properties common to them. On the other hand, it is unclear that the special property implicitly assumed in [20] holds for these BE schemes.

Note that our syntax of AtBE and properties cannot be trivially obtained from Kiayias and Samari's results.

We also present lower bounds on the authenticator size required for ABA by taking a similar approach to ANO-BE's one. Our lower bounds on the authenticator size are $\Omega(|\mathcal{S}| \cdot \kappa)$ and $\Omega(N \cdot \kappa)$ for BA with anonymity (ANO-BA) or full anonymity (Full-ANO-BA), respectively. These are asymptotically tight as there exists concrete ABA schemes proposed in [37] that meet our lower bounds on the authenticator size. There are several broadcast authentication protocols [7, 32, 33] including TESLA [34] with constant-sized authenticators. We cannot give a fair efficiency comparison between them and ABA since the existing protocols aim to broadcast information to *all* receivers and do not allow a sender to choose an arbitrary subset of receivers. Nevertheless, as in Anonymous BE, our results seem to show anonymity notions require large authenticator overheads depending on the number of designated or all recipients.

(Non-asymptotically) tight upper bounds and lower bounds In this work, we further aim to derive (non-asymptotically) tight upper bounds and lower bounds in Anonymous BE. First, we show that upper bounds on the ciphertext-size for ANO-BE and Full-ANO-BE are $|\mathcal{S}| \cdot \kappa + o(|\mathcal{S}| \cdot \kappa)$, $N \cdot \kappa + o(N \cdot \kappa)$, respectively. Throught this paper, we call a scheme *optimal* if a coefficient of a dominant term in the ciphertext-size is one. Li and Gong [24] proposed an optimal ANO-BE scheme where the ciphertext-size is $(|\mathcal{S}| + 6) \cdot \kappa$. On the other hand, there exists no optimal Full-ANO-BE scheme. The only Full-ANO-BE scheme explicitly described is Libert et al.'s one [25], and it has ciphertexts whose size is $N \cdot |\mathsf{pke.ct}| + |\sigma|$. Since any ciphertext-size in IND-CCA secure PKE must be at least $2 \cdot \kappa$ to the best of our knowldege, the most efficient Full-ANO-BE scheme in terms of the ciphertext-size has ciphertexts whose size is $2N \cdot \kappa + |\sigma|$. In this paper, we propose a Full-ANO-BE scheme where the ciphertext-size is $(N + 6) \cdot \kappa$ based on Li and Gong's ANO-BE scheme [24]. From our Full-ANO-BE scheme and ANO-BE scheme in [24], we show that the ciphertext-size in ANO-BE and Full-ANO-BE are upper bounded by $|\mathcal{S}| \cdot \kappa + o(|\mathcal{S}| \cdot \kappa)$, $N \cdot \kappa + o(N \cdot \kappa)$, respectively. A comparison of the ciphertext-size is given in Table 1.

We also show that lower bounds on the ciphertext-size for ANO-BE and Full-ANO-BE are $|\mathcal{S}| \cdot \kappa + o(|\mathcal{S}| \cdot \kappa)$, $N \cdot \kappa + o(N \cdot \kappa)$, respectively. In computationally secure cryptographic constructions, especially in algebraic ones, a coefficient of a dominant term in ciphertext-sizes is greater than or equal to 1 since each parameter depends on the number of group elements (see, for example, [39]). Therefore, the coefficient of the dominant term in our asymptotic lower bounds can also be regarded as 1 or higher. Then, from the above upper bounds and the asymptotic lower bounds, we also show that the ciphertext-size for ANO-BE and Full-ANO-BE are lower bounded by $|\mathcal{S}| \cdot \kappa + o(|\mathcal{S}| \cdot \kappa)$, $N \cdot \kappa + o(N \cdot \kappa)$, respectively.

In addition, we apply a similar discussion as above to anonymous broadcast authentication (ABA). In this paper, we propose optimal constructions of ABA with anonymity and full anonymity, respectively. Table 2 shows a comparison of the authenticator size. Finally, via the

Table 1 A comparison of the ciphertext-size between (Full-)ANO-BE schemes

Scheme	$\lvert\mathsf{ct}_{\mathcal{S}}\rvert$	Security
[24]	$(\lvert\mathcal{S}\rvert + 6) \cdot \kappa$	Anonymity
[25]	$N \cdot \lvert\mathsf{pke.ct}\rvert + \lvert\mathsf{ots.sig}\rvert$	Full-anonymity
Ours	$(N + 6) \cdot \kappa$	Full-anonymity

Let $\lvert\mathcal{S}\rvert$ and N be the size of a recipient set $\mathcal{S}$ and the number of all users in a system, respectively. $\lvert\mathsf{pke.ct}\rvert$ and $\lvert\mathsf{ots.sig}\rvert$ denote the ciphertext-size in IND-CCA secure PKE and the signature-size in sUF-CMA secure one-time signature, respectively. Note that Libert et al.'s scheme [25, Sect. 3.1] meets Full-Anonymity, though the original paper [25] only mentioned that it satisfies Anonymity

Table 2 A comparison of the authenticator size between ABA schemes

Scheme	$\lvert\mathsf{cmd}_{\mathcal{S}}\rvert$	Security
[37]	$(2\lvert\mathcal{S}\rvert + 2) \cdot \kappa$	Anonymity
Ours	$(\lvert\mathcal{S}\rvert + 2) \cdot \kappa$	Anonymity
[37]	$(2N + 2) \cdot \kappa$	Full-anonymity
Ours	$(N + 2) \cdot \kappa$	Full-anonymity

Let $\lvert\mathcal{S}\rvert$ and N be the size of a recipient set $\mathcal{S}$ and the number of all users in a system, respectively

same analysis as ANO-BE, we show that lower bounds and upper bounds on the authenticator size for ABA to satisfy anonymity and full anonymity are $\lvert\mathcal{S}\rvert \cdot \kappa + o(\lvert\mathcal{S}\rvert \cdot \kappa)$, $N \cdot \kappa + o(N \cdot \kappa)$, respectively.

Differences from the conference paper [22] This paper is an extended version of the conference version [22]. First, since the proof of Lemma 1 in the conference version [22] has a fatal flaw, we revisit a way to prove the lower bounds. Specifically, we restate the lemma (see Lemma 2 in Sect. 4) in a computational-security sense, i.e., there is no probabilistic polynomial-time adversary to find secret keys that fulfil a certain condition, while the lemma in [22] deals with adversaries with unbounded computational power. Second, we additionally show (non-asymptotically) tight lower bounds and upper bounds while the conference version [22] covers only asymptotically tight lower bounds.

1.2 Technical overview

Kiayias and Samari's approach [20] Kiayias and Samari provided a lower bound on the number of sub-elements in a BE ciphertext, not the bit length of the ciphertexts. To make it easier to deal with the sub-elements, they introduced AtBE where ciphertexts and decryption keys are composed of atomic ciphertexts and decryption keys. In more details, a ciphertext $\mathsf{ct}_{\mathcal{S}}$ consists of ρ atomic ciphertexts $\mathsf{ct}_{\mathcal{S}}^{(1)}, \ldots, \mathsf{ct}_{\mathcal{S}}^{(\rho)}$, and a decryption key for a recipient id consists of τ atomic decryption keys $\mathsf{sk}_{\mathsf{id}}^{(1)}, \ldots, \mathsf{sk}_{\mathsf{id}}^{(\tau)}$, respectively. If the recipient id is included in $\mathcal{S}$, there exists at least one pair of an atomic ciphertext $\mathsf{ct}_{\mathcal{S}}^{(\theta)}$ and decryption key $\mathsf{sk}_{\mathsf{id}}^{(\gamma)}$ that produces a message m (i.e., $\mathsf{ct}_{\mathcal{S}}^{(\theta)}$ can be decrypted with $\mathsf{sk}_{\mathsf{id}}^{(\gamma)}$).

They then analyzed a lower bound on the number of the atomic ciphertexts in any anonymous AtBE scheme. More specifically, they showed in [20, Theorem 2] that "for any AtBE scheme, if there exists a set $\mathcal{S}$ such that the number of atomic ciphertexts in $\mathsf{ct}_{\mathcal{S}}$ is smaller than

$|\mathcal{S}|$, then there is a successful adversary against anonymity for the AtBE scheme." However, the following property was implicitly assumed for AtBE in their proof:

Assumption 1 For all messages m, all privileged sets $\mathcal{S} \subseteq \mathcal{ID}$, let $\{\mathsf{ct}_{\mathcal{S}}^{(\theta)}\}_{\theta\in[\rho]} = \mathsf{ct}_{\mathcal{S}} \leftarrow \mathsf{Enc}(\mathsf{pk}, \mathsf{m}, \mathcal{S})$, where $\mathcal{ID}$ is the set of all recipients. For all $\mathsf{id}, \mathsf{id}' \in \mathcal{S}$, if they can decrypt the same atomic ciphertext $\mathsf{ct}_{\mathcal{S}}^{(\theta)}$ contained in $\mathsf{ct}_{\mathcal{S}}$, then atomic decryption keys $\mathsf{sk}_{\mathsf{id}}^{(\gamma)}$ and $\mathsf{sk}_{\mathsf{id}'}^{(\gamma')}$ used for the decryption are identical.

Namely, they indeed proved "for any AtBE scheme, if Assumption 1 holds (i.e., the AtBE scheme has the above property) and there exists a set $\mathcal{S}$ such that the number of atomic ciphertexts in $\mathsf{ct}_{\mathcal{S}}$ is less than $|\mathcal{S}|$, then there is an adversary which can break (full) anonymity for the AtBE scheme." However, it is difficult to check whether the above property holds for the Anonymous BE schemes; in any existing Anonymous BEs [3, 20, 24, 25], a situation where "any two recipients $\mathsf{id}, \mathsf{id}' \in \mathcal{S}$ decrypt the same atomic ciphertext $\mathsf{ct}_{\mathcal{S}}^{(\theta)}$ contained in $\mathsf{ct}_{\mathcal{S}}$" never occurs. Here, the contraposition of their theorem is "for any AtBE scheme, if it satisfies (full) anonymity, then Assumption 1 does not hold, or the number of atomic ciphertext in $\mathsf{ct}_{\mathcal{S}}$ is greater than or equal to $|\mathcal{S}|$ for all privileged set $\mathcal{S}$." In other words, the lower bound holds only if an AtBE scheme satisfies anonymity and Assumption 1 holds. For this reason, their proof is insufficient to show that their lower bound is asymptotically tight, since it is unclear whether Assumption 1 holds for existing (Anonymous) BE schemes. Note that the special property may not be removed from their proof trivially since it enables their attacker to break (full) anonymity for the AtBE scheme.

Our approach We avoid the problem by developing Kiayias and Samari's analysis. We consider other properties common to existing (Anonymous) BE schemes and derive a lower bound with them instead of the special property. To do so, we newly give a formal definition of AtBE so that these properties can be described formally, while Kiayias and Samari only presented AtBE in an informal way. Our AtBE allows a public key pk to be divided into several sub-elements, called *atomic public keys* $\mathsf{pk}^{(1)}, \ldots, \mathsf{pk}^{(\Delta)}$, as well as a ciphertext and a secret key. It also has Enc and Dec which are the same as ones of BE, and $\mathsf{Enc\text{-}at}$ and $\mathsf{Dec\text{-}at}$ algorithms to represent encryption and decryption procedures for each atomic ciphertext in the Enc and Dec algorithms of BE, respectively. In the $\mathsf{Enc\text{-}at}$, multiple atomic public keys $\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta'}$ are used to generate an atomic ciphertext $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$ corresponding to a recipient id in $\mathcal{S}$, where $\Delta' \subseteq \Delta$. In the $\mathsf{Dec\text{-}at}$, an atomic ciphertext $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$ is decrypted using multiple atomic decryption keys $\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma'_{\mathsf{id}}}$. Note that almost all (even non-Anonymous) BE schemes [1–3, 5, 6, 15, 16, 20, 24, 25, 30, 38] indeed have these algorithms inside the Enc and Dec. We then formalize the following four properties of our AtBE:

1. When a ciphertext has an intended recipient set $\mathcal{S}$, then any recipient in $\mathcal{S}$ can obtain the underlying message by decrypting at least one of the corresponding atomic ciphertexts.
2. A triplet of a recipient, recipient set, and message $(\mathsf{id}, \mathcal{S}, \mathsf{m})$ uniquely determines the minimum subset of atomic public keys required to generate an atomic ciphertext $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$.
3. A pair of a recipient and recipient set $(\mathsf{id}, \mathcal{S})$ uniquely determines the minimum subset of atomic decryption keys required to decrypt a (correctly-generated) atomic ciphertext $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$.
4. If two atomic ciphertexts $\mathsf{ct}_{\mathcal{S},\mathsf{id}}, \mathsf{ct}_{\mathcal{S},\mathsf{id}'}$ are identical, then the two corresponding minimum subsets of atomic public keys generating $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$ and $\mathsf{ct}_{\mathcal{S},\mathsf{id}'}$ are also identical.

In Sect. 3.2, we show that most existing BE schemes satisfy the above four properties.

Next, we explain how to provide a lower bound on ciphertext-sizes in Anonymous BE with those properties. In our approach, we derive a neccesary condition for AtBE schemes

with the properties to meet (full) anonymity while Kiayias and Samari directly prove the contraposition of "if an AtBE scheme is (full) anonymous, then the lower bound holds". Roughly speaking, we show the following necessary condition:

Lemma 2 (Informal, see Sect. 4) *Suppose an AtBE scheme satisfies the four properties, and fix an arbitrary recipient set $|\mathcal{S}|$ and an arbitrary ciphertext $\mathsf{ct}_{\mathcal{S}}$. Then, though a part of atomic decryption keys might overlap among recipients in $|\mathcal{S}|$, the minimum subsets of atomic decryption keys used to decrypt $\mathsf{ct}_{\mathcal{S}}$ are different for all designated recipients.*

We then prove that "for any AtBE scheme, if the lower bound does not hold, then the neccesary condition also does not hold (i.e., the AtBE does not meet anonymity)". See Theorem 1 in Sect. 4 for the formal statement. Here, instead of Assumption 1, we assume the following property that most Anonymous BEs have [3, 24, 25] to prove Theorem 1:

Assumption 2 For any $\mathcal{S} \subset \mathcal{ID}$, any $\mathsf{id} \in \mathcal{S}$, and any m, let pk' be a subset of atomic public keys that produces $\mathsf{ct}_{\mathcal{S},\mathsf{id}} \leftarrow \mathsf{Enc\text{-}at}(\mathsf{pk}', \mathcal{S}, \mathsf{m}, \mathsf{id})$. Then, pk' uniquely determines a minimum subset of atomic decryption keys required to decrypt $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$.

Note that, unlike Assumption 1, one can easily check if Assumption 2 holds for all existing Anonymous BEs [3, 24, 25]. Also, we handle the above property as an assumption since it does not hold for most of existing non-Anonymous BE schemes. Finally, we prove that for any AtBE scheme satisfies the four properties and Assumption 2, if there exists a set $\mathcal{S}$ such that the number of atomic ciphertexts in $\mathsf{ct}_{\mathcal{S}}$ is smaller than $|\mathcal{S}|$, then it contradicts the neccesary condition (Lemma 3 in Sect. 4).

2 Preliminaries

2.1 Notations

For all natural number $n \in \mathbb{N}$, $\{1, \ldots, n\}$ is denoted by $[n]$. For a finite set $\mathcal{X}$, we denote by $|\mathcal{X}|$ the cardinality of $\mathcal{X}$. For finite sets $\mathcal{X}, \mathcal{Y}$, let $\mathcal{X} \triangle \mathcal{Y}$ be the symmetric difference $\mathcal{X} \triangle \mathcal{Y} := (\mathcal{X} \backslash \mathcal{Y}) \cup (\mathcal{Y} \backslash \mathcal{X})$. For any finite set $\mathcal{X}$ and any natural number $N \in \mathbb{N}$, let $2^{\mathcal{X}}_{\leq N} := \{\mathcal{Y} \subset \mathcal{X} \mid |\mathcal{Y}| \leq N\}$ be the family of subsets of $\mathcal{X}$ whose cardinality is at most N (i.e., a part of a power set of $\mathcal{X}$). For any algorithm A, $\mathsf{out} \leftarrow \mathsf{A}(\mathsf{in})$ means that A takes in as input and outputs out. For any set $\mathcal{X}$, if we write $x \xleftarrow{\mathsf{U}} \mathcal{X}$, x is chosen uniformly at random from $\mathcal{X}$. For any distribution $\mathcal{D}$, if we write $d \xleftarrow{\mathsf{U}} \mathcal{D}$, d is chosen uniformly at random from $\mathcal{D}$ that is uniform over some set. Throughout our paper, we denote a security parameter by κ and consider probabilistic polynomial-time (PPT). For any element $x \in \{0, 1\}^*$, let $|x|$ be the number of bits of x. We say a positive-valued function $\mathsf{negl}(\cdot)$ is negligible if for any polynomial $\mathsf{poly}(\cdot)$, there exists some constant κ_0, such that $\mathsf{negl}(\kappa) < 1/\mathsf{poly}(\kappa)$ for all $\kappa \geq \kappa_0$.

2.2 Prime order bilinear groups and cryptographic assumption

Prime-order group A group generator GGen is a PPT algorithm which takes security parameter 1^κ as input and outputs a description $\mathcal{G} := (\mathsf{p}, \mathbb{G}, \mathsf{g})$. Here $\mathbb{G}$ is a finite cyclic group of prime order p and g is a random generator of $\mathbb{G}$. For $a \in \mathbb{Z}_p$ and a matrix $\mathbf{A} = (a_{ij}) \in \mathbb{Z}_p^{m \times n}$, we define the *implicit representation* [9] as $[a] := \mathsf{g}^a \in \mathbb{G}$ and $[\mathbf{A}] = (\mathsf{g}^{a_{ij}}) \in \mathbb{G}^{m \times n}$.

Prime-order bilinear groups A group generator PGGen is a PPT algorithm which takes security parameter 1^κ as input and outputs a description $\mathcal{PG} := (\mathsf{p}, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, \mathsf{g}_1, \mathsf{g}_2)$ of bilinear groups. Here $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ are finite cyclic groups of prime order p and $\mathsf{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is a (non-degenerate, efficiently computable) bilinear map. $\mathsf{g}_1 \in \mathbb{G}_1$ and $\mathsf{g}_2 \in \mathbb{G}_2$ are random generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, and $\mathsf{g}_T := \mathsf{e}(\mathsf{g}_1, \mathsf{g}_2)$ will be a generator of group $\mathbb{G}_T$. The bilinear map e is called *symmetric* in the case of $\mathbb{G}_1 = \mathbb{G}_2$, and *asymmetric* in the case of $\mathbb{G}_1 \neq \mathbb{G}_2$. In the case of symmetric, we let the description be $\mathcal{PG} := (\mathsf{p}, \mathbb{G}, \mathbb{G}_T, \mathsf{e}, \mathsf{g})$, where $\mathsf{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. In this paper, unless otherwise noted, we consider case $\mathbb{G}_1 \neq \mathbb{G}_2$. For $a \in \mathbb{Z}_p$, we define the *implicit representation* [9] as $[a]_s := \mathsf{g}_s^a \in \mathbb{G}_s$ where $s \in \{1, 2, T\}$. We let $\mathsf{e}([\mathbf{A}]_1, [\mathbf{B}]_2) := [\mathbf{AB}]_T$ for matrices $\mathbf{A}$ and $\mathbf{B}$ when the multiplication is well-defined.[5]

Cryptographic assumptions For any $k \in \mathbb{N}$, we call $\mathcal{D}_k$ a matrix distribution if it outputs full-rank matrices in $\mathbb{Z}_p^{(k+1)\times k}$ in polynomial time. We assume that for all $\mathbf{A} \xleftarrow{\cup} \mathcal{D}_k$, the first k rows of $\mathbf{A}$ form an invertible matrix.

We will use $\mathcal{D}_k$-Matrix Diffie–Hellman ($\mathcal{D}_k$-MDDH) assumption [9] and $\mathcal{D}_k$-Kernel Matrix Diffie–Hellman ($\mathcal{D}_k$-KerMDH) assumption [29] to construct Full-ANO-BE scheme. As discussed in [9] and [29], these assumptions are known to be standard and reasonable, and widely used to construct PKE [13, 14, 18, 26] and IBE [4, 17, 19, 23]. They are also used in [24] in the context of Anonymous Broadcast Encryption.

Assumption1 ($\mathcal{D}_k$-**MDDH**) [9] We say that the $\mathcal{D}_k$-Matrix Diffie–Hellman assumption holds relative to GGen, if for any PPT algorithm A, the following advantage function is negligible in κ.

$$\mathsf{Adv}^{\mathsf{mddh}}_{\mathsf{A},\mathbb{G}}(1^\kappa) := |\Pr[\mathsf{A}(\mathcal{G}, [\mathbf{A}], [\mathbf{As}]) = 1] - \Pr[\mathsf{A}(\mathcal{G}, [\mathbf{A}], [\mathbf{u}] = 1]|$$

where $\mathcal{G} \xleftarrow{\cup} \mathsf{GGen}(1^\kappa)$, $\mathbf{A} \xleftarrow{\cup} \mathcal{D}_k$, $\mathbf{s} \xleftarrow{\cup} \mathbb{Z}_p^k$, and $\mathbf{u} \xleftarrow{\cup} \mathbb{Z}_p^{k+1}$.

Assumption2 ($\mathcal{D}_k$-**KerMDH**) [29] Let $s \in \{1, 2\}$. We say that the $\mathcal{D}_k$-Kernel Matrix Diffie–Hellman Assumption holds relative to PGGen, if for any PPT algorithm A, the following advantage function is negligible in κ.

$$\mathsf{Adv}^{\mathsf{kddh}}_{\mathsf{A},\mathbb{G}_s}(1^\kappa) := \left|\Pr\left[\mathbf{A}^\top \mathbf{a}^\perp \wedge \mathbf{a}^\perp \neq \mathbf{0} \,\middle|\, \left[\mathbf{a}^\perp\right]_{3-s} \leftarrow \mathsf{A}(\mathbb{G}, [\mathbf{A}]_s)\right]\right|$$

where $\mathcal{PG} \xleftarrow{\cup} \mathsf{PGGen}(1^\kappa)$, $\mathbf{A} \xleftarrow{\cup} \mathcal{D}_k$.

2.3 Cryptographic primitives

Symmetric key encryption A symmetric key encryption (SKE) scheme with a key space $\mathcal{K}$ consists of two algorithms $\Pi^{\mathsf{SKE}} = (\mathsf{E}, \mathsf{D})$:

- $\mathsf{c} \leftarrow \mathsf{E}_\mathsf{K}(\mathsf{m})$: the encryption algorithm generates a ciphetext c of the message m under the secret key $\mathsf{K} \in \mathcal{K}$. Here, $\mathcal{K}$ is a secret key space.
- $\mathsf{m} \leftarrow \mathsf{D}_\mathsf{K}(\mathsf{c})$: the decryption algorithm decrypts the ciphertext c using K, and returns $\mathsf{m} \in \mathcal{M} \cup \{\perp\}$.

Correctness For all $\mathsf{K} \in \mathcal{K}$ and all message m, we have $\mathsf{D}_\mathsf{K}(\mathsf{E}_\mathsf{K}(\mathsf{m})) = \mathsf{m}$ with overwhelming probability.

[5] In the case of symmetric, $\mathsf{e}([\mathbf{B}]_2, [\mathbf{A}]_1) := [\mathbf{BA}]_T$ is also allowed.

Definition 1 (Semantic Security) A SKE scheme is semantically secure, if for all PPT adversary A, the following advantage function is negligible in κ.

$$\mathsf{Adv}^{\mathsf{se}}_{\mathsf{A}}(\kappa) := \left| \Pr\left[b' = b \;\middle|\; \begin{array}{l} (\mathsf{m}_0, \mathsf{m}_1) \leftarrow \mathsf{A}(\kappa, \mathcal{K}), \\ \mathsf{K} \xleftarrow{\mathsf{U}} \mathcal{K}, b \xleftarrow{\mathsf{U}} \{0,1\}, \\ \mathsf{c}^* \leftarrow \mathsf{E}_{\mathsf{K}}(\mathsf{m}_b), \\ b' \leftarrow \mathsf{A}(1^\kappa, \mathcal{K}, \mathsf{c}^*) \end{array} \right] - \frac{1}{2} \right|.$$

Furthermore, we require the symmetric encryption to be key-binding [12]. Namely, for any message m and any secret key $\mathsf{K} \in \mathcal{K}$, there exists no key $\mathsf{K}' \in \mathcal{K}$ such that $\mathsf{K}' \neq \mathsf{K}$ and $\mathsf{D}_{\mathsf{K}'}(\mathsf{E}_{\mathsf{K}}(\mathsf{m})) \neq \perp$.

Collision-resilient hash function Let $\mathcal{H}$ be a family of hash functions $\mathsf{H} : \mathcal{X} \to \mathcal{Y}$. Here, $\mathcal{X} := \mathcal{X}_\kappa, \mathcal{Y} := \mathcal{Y}_\kappa$ are finite sets, respectively. $\mathcal{H}$ is said to be collision-resistant if, for all PPT algorithm A, the following advantage function is negligible in κ.

$$\mathsf{Adv}^{\mathsf{hash}}_{\mathsf{A}}(\kappa) := \Pr\left[\mathsf{H}(x) = \mathsf{H}(y) \wedge x \neq y \;\middle|\; \mathsf{H} \xleftarrow{\mathsf{U}} \mathcal{H}, (x, y) \leftarrow \mathsf{A}(1^\kappa, \mathsf{H}) \right].$$

Message authentication code A message authentication code (MAC) scheme consists of three algorithms $\Pi^{\mathsf{MAC}} = (\mathsf{MAC.Gen}, \mathsf{MAC.Auth}, \mathsf{MAC.Vrfy})$:

- $\mathsf{K} \leftarrow \mathsf{MAC.Gen}(1^\kappa)$: the key generation algorithm takes secruity parameter κ as inputs, and outputs a symmetric key K.
- $\tau \leftarrow \mathsf{MAC.Auth}(\mathsf{K}, \mathsf{m})$: the authentication algorithm takes K and a message $\mathsf{m} \in \mathcal{M}$ as inputs, and outputs an authentication tag $\tau \in \mathcal{T}$. Here, $\mathcal{M}$ is a message space and $\mathcal{T}$ is a tag space.
- $\top / \perp \leftarrow \mathsf{MAC.Vrfy}(\mathsf{K}, \tau, \mathsf{m})$: the verification algorithm takes K, τ and m as inputs, and outputs $\top$ (accept) or $\perp$ (reject).

Correctness For all $\kappa \in \mathbb{N}$, all $\mathsf{K} \leftarrow \mathsf{MAC.Gen}(1^\kappa)$ and all message $\mathsf{m} \in \mathcal{M}$, we have $\mathsf{MAC.Vrfy}(\mathsf{K}, \mathsf{MAC.Auth}(\mathsf{K}, \mathsf{m})) \to \top$ with overwhelming probability.

We define unforgeability against chosen message attack (UF-CMA) in a multi-key setting [28]. Let A be any PPT adversary against UF-CMA security. We consider an experiment $\mathsf{Exp}^{\mathsf{UF\text{-}CMA}}_{\Pi^{\mathsf{MAC}},\mathsf{A}}(\kappa)$ between a challenger C and A as follows.

$\mathsf{Exp}^{\mathsf{UF\text{-}CMA}}_{\Pi^{\mathsf{MAC}},\mathsf{A}}(\kappa)$

C runs $\mathsf{MAC.Gen}(1^\kappa)$ to get $(\mathsf{K}_1, \ldots, \mathsf{K}_{\ell(\kappa)})$. Let $\widetilde{\mathcal{M}}, \mathcal{I}$ be empty sets and flag be a flag, where flag is initialized as 1. We denote $\widetilde{\mathcal{M}}$ as a set of messages used for authentication queries. $\mathcal{I}$ as a set of indexes used for key derivation queries. A may adaptively issue an authentication query $(\mathsf{id}, \mathsf{m}) \in \ell(\kappa) \times \mathcal{M}$ to Authentication Oracle Auth, and Auth returns $\tau \leftarrow \mathsf{MAC.Auth}(\mathsf{K}_{\mathsf{id}}, \mathsf{m})$, then adds $(\mathsf{id}, \mathsf{m})$ to $\widetilde{\mathcal{M}}$. Also, A may adaptively issue a key derivation query $\mathsf{id} \in \ell(\kappa)$ to Key Derivation Oracle Corr, and Corr returns K_{id}, then adds id to $\mathcal{I}$. Finally, A issues a verification query $(\mathsf{m}^*, \tau^*, \mathsf{id}^*)$ to Verification Oracle Vrfy. At this point, if $\mathsf{id}^* \in \mathcal{I}$ or $(\mathsf{id}^*, \mathsf{m}^*) \in \widetilde{\mathcal{M}}$ or $\perp \leftarrow \mathsf{MAC.Vrfy}(\mathsf{K}_{\mathsf{id}^*}, \tau^*, \mathsf{m}^*)$ holds, then C sets $\mathsf{flag} := 0$ For simplicity, A is restricted to issue this query only once. At some point (right after some verification query without loss of generality), A terminates the experiment, and C sets flag as the output of $\mathsf{Exp}^{\mathsf{UF\text{-}CMA}}_{\Pi^{\mathsf{MAC}},\mathsf{A}}(\kappa)$.

Definition 2 (UF-CMA) We say Π^{MAC} is UF-CMA secure if for any PPT adversary A, for all sufficiently-large $\kappa \in \mathbb{N}$, it holds that $\mathsf{Adv}^{\mathsf{UF\text{-}CMA}}_{\Pi^{\mathsf{MAC}},\mathsf{A}}(\kappa) < \mathsf{negl}(\kappa)$, where $\mathsf{Adv}^{\mathsf{UF\text{-}CMA}}_{\Pi^{\mathsf{MAC}},\mathsf{A}}(\kappa) := \Pr\left[\mathsf{Exp}^{\mathsf{UF\text{-}CMA}}_{\Pi^{\mathsf{MAC}},\mathsf{A}}(\kappa) \to 1\right]$.

2.4 Core Lemma

We will use the core lemma [21], which was originally used to prove adaptive soundness of quasi-adaptive non-interactive zero-knowledge (QANIZK) proofs, to prove security of our Full-ANO-BE scheme in Sect. 5. We review a slightly simplified version of the core lemma below since it is sufficient for our purpose.

Lemma 1 (Core lemma [21]) *Let $k \in \mathbb{N}$. For any $\mathbf{A}, \mathbf{B} \in \mathbb{Z}_p^{(k+1)\times k}$ and any (possibly unbounded) adversary A, we have*

$$\Pr\left[\begin{array}{l|l} \mathbf{u} \notin \mathrm{span}(\mathbf{A}) \wedge \alpha \neq \alpha^* & \mathbf{X}, \mathbf{Y} \xleftarrow{\cup} \mathbb{Z}_p^{(k+1)\times(k+1)} \\ \wedge\, \boldsymbol{\pi}^\top = \mathbf{u}^\top(\mathbf{X} + \alpha \cdot \mathbf{Y}) & (\mathbf{u}, \alpha, \boldsymbol{\pi}) \leftarrow \mathsf{A}^{O(\cdot)}(\mathbf{A}^\top\mathbf{X}, \mathbf{A}^\top\mathbf{Y}, \mathbf{XB}, \mathbf{YB}) \end{array}\right] \leq \frac{1}{p},$$

where $(\mathbf{u}, \alpha, \boldsymbol{\pi}) \in \mathbb{Z}_p^{k+1} \times \mathbb{Z}_p \times \mathbb{Z}_p^k$, the span $\mathrm{span}(\mathbf{A})$ of a matrix $\mathbf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_k)$ means the span of the vectors $\mathbf{a}_1, \ldots, \mathbf{a}_k$, A can issue $\alpha^* \in \mathbb{Z}_p$ to oracle O, which returns $\mathbf{X} + \alpha^* \cdot \mathbf{Y}$, only once.

2.5 Broadcast encryption

We define Broadcast Encryption (BE) and its security notions based on [25, 37]. In this paper, we assume that the maximum number of recipients N in BE is determined at the time of setup and an arbitrary set of recipients can be specified at the time of encryption.

Syntax A BE scheme Π^{BE} consists of four algorithms $(\mathsf{Setup}, \mathsf{Join}, \mathsf{Enc}, \mathsf{Dec})$.

1. $(\mathsf{mk}, \mathsf{pk}) \leftarrow \mathsf{Setup}(1^\kappa, N)$: a probabilistic algorithm for setup. It takes a security parameter 1^κ and the maximum number of recipients $N \in \mathbb{N}$ as input, and outputs a master secret key mk and a public key pk.
2. $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{Join}(\mathsf{mk}, \mathsf{id})$: a decryption key generation algorithm. It takes mk and an identifier $\mathsf{id} \in \mathcal{ID}$, as input, and outputs a decryption key $\mathsf{sk}_{\mathsf{id}}$ for id. Here, $\mathcal{ID}$ is a set of all possible identifiers, and $|\mathcal{ID}| := \mathsf{poly}(\kappa)$ for some polynomial $\mathsf{poly}(\cdot)$.
3. $\mathsf{ct}_{\mathcal{S}} \leftarrow \mathsf{Enc}(\mathsf{pk}, \mathsf{m}, \mathcal{S}; \mathsf{r})$: an encryption algorithm. It takes pk, a message $\mathsf{m} \in \mathcal{M}$, randomness $\mathsf{r} \in \mathcal{R}$, and a privileged set $\mathcal{S} \subseteq \mathcal{ID}$ as input, and outputs a ciphertext $\mathsf{ct}_{\mathcal{S}} \in \mathcal{CT}$, where $\mathcal{M}$ is a message-space, $\mathcal{CT}$ is a ciphetex-space and $\mathcal{R}$ is a randomness-space. It is also possible to omit r from the input.
4. $\mathsf{m} \leftarrow \mathsf{Dec}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct}_{\mathcal{S}})$: a decryption algorithm. It takes $\mathsf{sk}_{\mathsf{id}}$ and $\mathsf{ct}_{\mathcal{S}}$ as inputs, and outputs $\mathsf{m} \in \mathcal{M} \cup \{\perp\}$.

To describe properties of the existing Anonymous BE schemes, we regard Join as a deterministic algorithm in this paper.[6]

Correctness For all $\kappa, N \in \mathbb{N}$, all $\mathsf{mk} \leftarrow \mathsf{Setup}(1^\kappa, N)$, all $\mathsf{m} \in \mathcal{M}$, all $\mathsf{r} \in \mathcal{R}$, all $\mathcal{S} \subseteq \mathcal{ID}$ such that $|\mathcal{S}| \leq N$, and all $\mathsf{id} \in \mathcal{S}$, we have $\mathsf{m} \leftarrow \mathsf{Dec}(\mathsf{Join}(\mathsf{mk}, \mathsf{id}), \mathsf{Enc}(\mathsf{pk}, \mathsf{m}, \mathcal{S}; \mathsf{r}))$ with overwhelming probability.

Chosen ciphertext security and anonymity We define anonymity and indistinguishability against chosen ciphertext attack (Full-ANO-IND-CCA) for BE. We consider two anonymity notions, Full-ANO-IND-CCA [20, 37] and ANO-IND-CCA [24, 25] security. Let A be any PPT adversary against Full-ANO-IND-CCA security. Following [20, 24, 25, 37], we consider an experiment $\mathsf{Exp}^{\text{Full-}ANO\text{-IND-CCA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N)$ between a challenger C and A as follows.

[6] It does not affect our analysis since we can covert any probabilistic Join algorithm into a deterministic one by using a pseudo-random function.

$\mathsf{Exp}^{\text{Full-}ANO\text{-IND-CCA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N)$ C randomly chooses $b \in \{0,1\}$. C runs $\mathsf{Setup}(1^\kappa, N)$ to get mk and randomly chooses $b \in \{0,1\}$. Let $\mathcal{D}, \mathcal{CD}$ be empty sets. We denote $\mathcal{D}$ as a set of recipients currently participating in the protocol, and $\mathcal{CD}$ as a set of identifiers of recipient from which A obtained its decryption key, respectively. A may adaptively issue the following queries to C.

- Key-generation Query: Upon a query $\mathsf{id} \in \mathcal{ID}$ from A, C adds id to $\mathcal{D}$ and generates $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{Join}(\mathsf{mk}, \mathsf{id})$. Note that A obtains nothing, and that A is allowed to make this query at most N times.
- Corruption Query: Upon a query $\mathsf{id} \in \mathcal{D}$ from A, C adds id to $\mathcal{CD}$, and returns $\mathsf{sk}_{\mathsf{id}}$ to A.
- Challenge Query: Upon a query $(\mathsf{m}_0, \mathsf{m}_1, \mathcal{S}_0, \mathcal{S}_1) \in \mathcal{M}^2 \times \left(2^{\mathcal{D}}_{\leq N}\right)^2$ from A, C runs $\mathsf{ct}^*_{\mathcal{S}} \leftarrow \mathsf{Enc}(\mathsf{pk}, \mathsf{m}_b, \mathcal{S}_b)$ and returns $\mathsf{ct}_{\mathcal{S}}$ to A. A is allowed to make this query only.
- Decryption Query: Upon a query $(\mathsf{id}, \mathsf{ct}_{\mathcal{S}}) \in \mathcal{D} \times \mathcal{CT}$ from A returns $\mathsf{m} \leftarrow \mathsf{Dec}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct}_{\mathcal{S}})$ to A. If $\mathsf{ct}^*_{\mathcal{S}}$ is queried, then returns $\perp$.

At some point, A outputs b'. If all of the following conditions hold C then sets 1 as the output of $\mathsf{Exp}^{\text{Full-}ANO\text{-IND-CCA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N)$:

- $b' = b$
- $|\mathsf{m}_0| = |\mathsf{m}_1|$
- $(\mathcal{S}_0 \triangle \mathcal{S}_1) \cap \mathcal{CD} = \emptyset$
- If $(\mathcal{S}_0 \triangle \mathcal{S}_1) \cap \mathcal{CD} \neq \emptyset$, then $\mathsf{m}_0 = \mathsf{m}_1$

Otherwise, C then sets 0. C terminates the experiment.
We can also define ANO-IND-CCA with an experiment $\mathsf{Exp}^{\text{ANO-IND-CCA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N)$ which is the same as $\mathsf{Exp}^{\text{Full-}ANO\text{-IND-CCA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N)$ except for the following additional condition of the restriction for challenge query: $|\mathcal{S}_0| = |\mathcal{S}_1|$.

Definition 3 ((Full-)ANO-IND-CCA) We say Π^{BE} is X-CCA secure (X $\in$ {Full-ANO-IND, ANO-IND}) secure if for any PPT adversary A, for all sufficiently-large $\kappa \in \mathbb{N}$ and all $N \in \mathbb{N}$, it holds that $\mathsf{Adv}^X_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N) < \mathsf{negl}(\kappa)$, where $\mathsf{Adv}^X_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N) := \left|\Pr\left[\mathsf{Exp}^X_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N) \to 1\right] - \frac{1}{2}\right|$.

The third and fourth conditions are intended to prevent the trivial attack when a decryption key of a user $\mathsf{id} \in \mathcal{S}_0 \triangle \mathcal{S}_1$ is corrupted.
We also define IND-CCA with an experiment $\mathsf{Exp}^{\text{IND-CCA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N)$ which is the same as $\mathsf{Exp}^{\text{ANO-IND-CCA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N)$, except for the following additional condition of the restriction for challenge query: $\mathcal{S}_0 = \mathcal{S}_1$.

Definition 4 (IND-CCA) We say Π^{BE} is IND-CCA secure if for any PPT adversary A, for all sufficiently-large $\kappa \in \mathbb{N}$ and all $N \in \mathbb{N}$, it holds that $\mathsf{Adv}^{\text{IND-CCA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N) < \mathsf{negl}(\kappa)$, where $\mathsf{Adv}^{\text{IND-CCA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N) := \left|\Pr\left[\mathsf{Exp}^{\text{IND-CCA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N) \to 1\right] - \frac{1}{2}\right|$.

Also, (Full-)ANO-CCA can be defined with experiments $\mathsf{Exp}^{\text{ANO-CCA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N)$ and $\mathsf{Exp}^{\text{Full-ANO-CCA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N)$ which are the same as $\mathsf{Exp}^{\text{ANO-IND-CCA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N)$ and $\mathsf{Exp}^{\text{Full-}ANO\text{-IND-CCA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N,)$ respectively, except for the following additional condition of the restriction for challenge query: $\mathsf{m}_0 = \mathsf{m}_1$.

Definition 5 ((Full-)ANO-CCA) We say Π^{BE} is X-CCA secure (X $\in$ {Full-ANO, ANO}) secure if for any PPT adversary A, for all sufficiently-large $\kappa \in \mathbb{N}$ and all $N \in \mathbb{N}$, it holds that $\mathsf{Adv}^X_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N) < \mathsf{negl}(\kappa)$, where $\mathsf{Adv}^X_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N) := \left|\Pr\left[\mathsf{Exp}^X_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N) \to 1\right] - \frac{1}{2}\right|$.

2.6 Anonymous broadcast authentication

We define Anonymous Broadcast Authentication (ABA) and its security notions based on [37].

Syntax An Anonymous Broadcast Authentication scheme Π^{ABA} consists of four algorithms $(\mathsf{Setup}, \mathsf{Join}, \mathsf{Auth}, \mathsf{Vrfy})$.

1. $\mathsf{ak} \leftarrow \mathsf{Setup}(1^\kappa, N)$: a probabilistic algorithm for setup. It takes a security parameter 1^κ and the maximum number of recipients $N \in \mathbb{N}$ as input, and outputs authentication key ak.
2. $\mathsf{vk}_{\mathsf{id}} \leftarrow \mathsf{Join}(\mathsf{ak}, \mathsf{id})$: a verification key generation algorithm. It takes ak and an identifier $\mathsf{id} \in \mathcal{ID}$, as input, and outputs verification key $\mathsf{vk}_{\mathsf{id}}$ for id. Here, $\mathcal{ID}$ is a set of all possible identifiers, and $|\mathcal{ID}| := \mathsf{poly}(\kappa)$ for some polynomial $\mathsf{poly}(\cdot)$.
3. $\mathsf{cmd}_{\mathcal{S}} \leftarrow \mathsf{Auth}(\mathsf{ak}, \mathsf{m}, \mathcal{S}; \mathsf{r})$: an authentication algorithm. It takes ak, a message $\mathsf{m} \in \mathcal{M}$, a randomness $\mathsf{r} \in \mathcal{R}$, and a privileged set $\mathcal{S} \subseteq \mathcal{ID}$ as input, and outputs ciphertext $\mathsf{cmd}_{\mathcal{S}}$, where $\mathcal{M}$ is a message space and $\mathcal{R}$ is a randomness space. It is also possible to omit r from the input.
4. $\mathsf{m}/\perp \leftarrow \mathsf{Vrfy}(\mathsf{vk}_{\mathsf{id}}, \mathsf{cmd}_{\mathcal{S}})$: a verification algorithm. It takes $\mathsf{vk}_{\mathsf{id}}$ and $\mathsf{cmd}_{\mathcal{S}}$ as inputs, and outputs $\mathsf{m} \in \mathcal{M}$ (accept) or $\perp$ (reject).

To describe properties of the existing ABA scheme, we regard Join as a deterministic algorithm in this paper.

Correctness For all $\kappa, N \in \mathbb{N}$, all $\mathsf{ak} \leftarrow \mathsf{Setup}(1^\kappa, N)$, all $\mathsf{m} \in \mathcal{M}$, all $\mathsf{r} \in \mathcal{R}$, and all $\mathcal{S} \subseteq \mathcal{ID}$ such that $|\mathcal{S}| \leq N$, if $\mathsf{id} \in \mathcal{S}$, then $\mathsf{m} \leftarrow \mathsf{Vrfy}(\mathsf{Join}(\mathsf{ak}, \mathsf{id}), \mathsf{Auth}(\mathsf{ak}, \mathsf{m}, \mathcal{S}))$ holds with overwhelming probability. Otherwise, $\perp \leftarrow \mathsf{Vrfy}(\mathsf{Join}(\mathsf{ak}, \mathsf{id}), \mathsf{Auth}(\mathsf{ak}, \mathsf{m}, \mathcal{S}))$ holds with overwhelming probability.

Unforgeability We define unforgeability against chosen message attack (UF-CMA) for ABA. Let A be any PPT adversary against UF-CMA security. We consider an experiment $\mathsf{Exp}^{\mathsf{UF\text{-}CMA}}_{\Pi^{\mathsf{ABA}},\mathsf{A}}(\kappa, N)$ between a challenger C and A.

$\mathsf{Exp}^{\mathsf{UF\text{-}CMA}}_{\Pi^{\mathsf{ABA}},\mathsf{A}}(\kappa, N)$

C runs $\mathsf{Setup}(1^\kappa, N)$ to get ak. Let $\mathcal{D}, \mathcal{CD}, \mathcal{M}_{\mathrm{A}}, \mathcal{M}_{\mathrm{V}}$ be empty sets and flag be a flag, where flag is initialized as 0. We denote $\mathcal{D}$ as a set of recipients currently participating in the protocol, and $\mathcal{CD}$ as a set of identifiers of recipient from which A obtained its verification key, respectively. And we denote $\mathcal{M}_{\mathrm{A}}, \mathcal{M}_{\mathrm{V}}$ as sets of messages used for authentication queries and verification queries, respectively. A may adaptively issue the following queries to C.

- Key-generation Query: Upon a query $\mathsf{id} \in \mathcal{ID}$ from A, C adds id to $\mathcal{D}$ and generates $\mathsf{vk}_{\mathsf{id}} \leftarrow \mathsf{Join}(\mathsf{ak}, \mathsf{id})$. Note that A obtains nothing, and that A is allowed to make this query at most N times.
- Corruption Query: Upon a query $\mathsf{id} \in \mathcal{D}$ from A, C adds id to $\mathcal{CD}$, and returns $\mathsf{vk}_{\mathsf{id}}$ to A.
- Authentication Query: Upon a query $(\mathsf{m}, \mathcal{S}) \in \mathcal{M} \times 2^{\mathcal{D}}_{\leq N}$ from A, C adds m to $\mathcal{M}_{\mathrm{A}}$, and returns $\mathsf{cmd}_{\mathcal{S}} \leftarrow \mathsf{Auth}(\mathsf{ak}, \mathsf{m}, \mathcal{S})$ to A if m is not used for a verification query ($\mathsf{m} \notin \mathcal{M}_{\mathrm{V}}$).
- Verification Query: Upon a query $(\mathsf{m}, \mathcal{S}, \mathsf{cmd}_{\mathcal{S}}) \in \mathcal{M} \times 2^{\mathcal{D}}_{\leq N} \times \mathcal{T}$ from A, C runs $\mathsf{Vrfy}(\mathsf{vk}_{\mathsf{id}}, \mathsf{cmd}_{\mathcal{S}})$ and returns its output to A. C adds m to $\mathcal{M}_{\mathrm{V}}$. If there exists at least one user $\mathsf{id} \in \mathcal{S}$ such that all of the following conditions hold, then C sets $\mathsf{flag} := 1$:
  - $\mathsf{Vrfy}(\mathsf{vk}_{\mathsf{id}}, \mathsf{cmd}_{\mathcal{S}}) = \mathsf{m}$,
  - $\mathsf{id} \notin \mathcal{CD}$,
  - $\mathsf{m} \notin \mathcal{M}_{\mathrm{A}}$.

  A is allowed to make this query only once.

At some point (right after some verification query without loss of generality), A terminates the experiment, and C sets flag as the output of $\mathsf{Exp}^{\mathsf{UF\text{-}CMA}}_{\Pi^{\mathsf{ABA}},\mathsf{A}}(\kappa)$.

Definition 6 (Unforgeability) We say Π^{ABA} is UF-CMA secure if for any PPT adversary A, for all sufficiently-large $\kappa \in \mathbb{N}$ and all $N \in \mathbb{N}$, it holds that $\mathsf{Adv}^{\mathsf{UF\text{-}CMA}}_{\Pi^{\mathsf{ABA}},\mathsf{A}}(\kappa, N) < \mathsf{negl}(\kappa)$, where $\mathsf{Adv}^{\mathsf{UF\text{-}CMA}}_{\Pi^{\mathsf{ABA}},\mathsf{A}}(\kappa, N) := \Pr\left[\mathsf{Exp}^{\mathsf{UF\text{-}CMA}}_{\Pi^{\mathsf{ABA}},\mathsf{A}}(\kappa, N) \to 1\right]$.

Anonymity We define two kinds of anonymity for ABA, full anonymity (Full-ANO-CMA) and anonymity (ANO-CMA). In this paper, we denote ABA with anonymity and ABA with full anonymity as ANO-BA and Full-ANO-BA, respectively. Let A be any PPT adversary against Full-ANO-CMA security. We consider an experiment $\mathsf{Exp}^{\mathsf{Full\text{-}ANO\text{-}CMA}}_{\Pi^{\mathsf{ABA}},\mathsf{A}}(\kappa, N)$ between a challenger C and A.

$\mathsf{Exp}^{\mathsf{Full\text{-}ANO\text{-}CMA}}_{\Pi^{\mathsf{ABA}},\mathsf{A}}(\kappa, N)$

C randomly chooses $b \in \{0, 1\}$. C runs $\mathsf{Setup}(1^\kappa, N)$ to get ak and randomly chooses $b \in \{0, 1\}$. Let $\mathcal{D}$, $\mathcal{CD}$, $\mathcal{M}_{\mathrm{A}}$ be empty sets. We denote $\mathcal{D}$ as a set of recipients currently participating in the protocol, and $\mathcal{CD}$ as a set of identifiers of recipient from which A obtained its verification key, respectively. And we denote $\mathcal{M}_{\mathrm{A}}$ as a set of messages used for authentication queries. A may adaptively issue the following queries to C.

- Key-generation Query: Upon a query $\mathsf{id} \in \mathcal{ID}$ from A, C adds id to $\mathcal{D}$ and generates $\mathsf{vk}_{\mathsf{id}} \leftarrow \mathsf{Join}(\mathsf{ak}, \mathsf{id})$. Note that A obtains nothing, and that A is allowed to make this query at most N times.
- Corruption Query: Upon a query $\mathsf{id} \in \mathcal{D}$ from A, C adds id to $\mathcal{CD}$, and returns $\mathsf{vk}_{\mathsf{id}}$ to A.
- Authentication Query: Upon a query $(\mathsf{m}, \mathcal{S}) \in \mathcal{M} \times 2^{\mathcal{D}}_{\leq N}$ from A, C adds m to $\mathcal{M}_{\mathrm{A}}$, and returns $\mathsf{cmd}_{\mathcal{S}} \leftarrow \mathsf{Auth}(\mathsf{ak}, \mathsf{m}, \mathcal{S})$ to A.
- Challenge Query: Upon a query $(\mathsf{m}, \mathcal{S}_0, \mathcal{S}_1) \in \mathcal{M} \times \left(2^{\mathcal{D}}_{\leq N}\right)^2$ from A, C runs $\mathsf{cmd}_{\mathcal{S}_b} \leftarrow \mathsf{Auth}(\mathsf{ak}, \mathsf{m}, \mathcal{S}_b)$ and returns $\mathsf{cmd}_{\mathcal{S}_b}$ to A. A is allowed to make this query only once under the restriction that $(\mathcal{S}_0 \triangle \mathcal{S}_1) \cap \mathcal{CD} = \emptyset$, $\mathsf{m} \notin \mathcal{M}_{\mathrm{A}}$.

At some point, A outputs b'. If $b' = b$, C then sets 1 as the output of $\mathsf{Exp}^{\mathsf{Full\text{-}ANO\text{-}CMA}}_{\Pi^{\mathsf{ABA}},\mathsf{A}}(\kappa, N)$. Otherwise, C then sets 0. C terminates the experiment.
We can also define ANO-CMA with an experiment $\mathsf{Exp}^{\mathsf{ANO\text{-}CMA}}_{\Pi^{\mathsf{ABA}},\mathsf{A}}(\kappa, N)$ which is the same as $\mathsf{Exp}^{\mathsf{Full\text{-}ANO\text{-}CMA}}_{\Pi^{\mathsf{ABA}},\mathsf{A}}(\kappa, N)$ except for the following additional condition of the restriction for challenge query: $|\mathcal{S}_0| = |\mathcal{S}_1|$.

Definition 7 (Anonymity) We say Π^{ABA} is X secure (X $\in$ {Full-ANO-CMA, ANO-CMA}) if for any PPT adversary A, for all sufficiently-large $\kappa \in \mathbb{N}$ and all $N \in \mathbb{N}$, it holds that $\mathsf{Adv}^{X}_{\Pi^{\mathsf{ABA}},\mathsf{A}}(\kappa, N) < \mathsf{negl}(\kappa)$, where $\mathsf{Adv}^{X}_{\Pi^{\mathsf{ABA}},\mathsf{A}}(\kappa, N) := \left|\Pr\left[\mathsf{Exp}^{X}_{\Pi^{\mathsf{ABA}},\mathsf{A}}(\kappa, N) \to 1\right] - \frac{1}{2}\right|$.

3 Atomic broadcast encryption

In this section, we give a formal syntax of Atomic Broadcast Encryption (AtBE) to formally describe properties satisfied by existing BE schemes. These properties are used to formalize properties of existing Anonymous BE schemes and derive lower bounds. We further provide security definitions for AtBE.

3.1 Syntax of AtBE

Our AtBE aims to describe encryption and decryption for each recipient in a designated set performed inside the Enc and Dec algorithms of BE. Towards that aim, ciphertexts, decryption keys, and public keys are divided into multiple sub-elements. An AtBE scheme $\Pi^{\mathsf{At\text{-}BE}}$ consists of six algorithms (Setup-at, Join-at, Enc, Enc-at, Dec, Dec-at), where the Enc and Dec are the same as ones of BE.

1. $(\mathsf{mk}, \{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta}) \leftarrow \mathsf{Setup\text{-}at}(1^\kappa, N)$: a probabilistic algorithm for setup. It takes a security parameter 1^κ and the maximum number of receivers $N \in \mathbb{N}$ as input, and outputs a master secret key mk and a public key pk consisting of $|\Delta|$ atomic public keys $\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta}$.
2. $\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma_{\mathsf{id}}} \leftarrow \mathsf{Join\text{-}at}(\mathsf{mk}, \mathsf{id})$: a decryption key generation algorithm. It takes mk and an identifier $\mathsf{id} \in \mathcal{ID}$, as input, and outputs a decryption key $\mathsf{sk}_{\mathsf{id}}$ for id consisting of $|\Gamma_{\mathsf{id}}|$ atomic decryption keys $\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma_{\mathsf{id}}}$.
3. $\mathsf{ct}_{\mathcal{S},\mathsf{id}} \leftarrow \mathsf{Enc\text{-}at}(\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta'}, \mathcal{S}, \mathsf{m}, \mathsf{id}; \mathsf{r})$: an atomic encryption algorithm. It takes a subset of the atomic public key $\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta'}$, a privileged set $\mathcal{S} \subseteq \mathcal{ID}$, a message $\mathsf{m} \in \mathcal{M}$, an identifier $\mathsf{id} \in \mathcal{ID}$, and randomness r as input, and outputs an atomic ciphertext $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$, where $\Delta' \subseteq \Delta$.
4. $\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma'_{\mathsf{id}}}, \mathsf{ct}_{\mathcal{S},\mathsf{id}})$: an atomic decryption algorithm. It takes a subset of atomic decryption keys $\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma'_{\mathsf{id}}}$, and $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$ as input, and outputs a message $\mathsf{m} \in \mathcal{M} \cup \{\perp\}$, where $\Gamma'_{\mathsf{id}} \subseteq \Gamma_{\mathsf{id}}$.

The Setup-at and Join-at are essentially equivalent to the Setup and Join in BE respectively, except for differences that public and decryption keys are explicitly divided into multiple sub-elements. As in the case of the Join in BE, we regard the Join-at as being a deterministic algorithm. On the other hand, the Enc and Dec include the Enc-at and Dec-at as sub-algorithms, respectively, though they might contain procedures other than the sub-algorithms. Therefore, AtBE includes both (Enc, Dec) and (Enc-at, Dec-at).

We require a natural property for AtBE that an atomic ciphertext $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$ contained in ciphertext $\mathsf{ct}_{\mathcal{S}}$ will be correctly decrypted by a decryption key $\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma_{\mathsf{id}}}$ of a recipient $\mathsf{id} \in \mathcal{S}$ as follows:

Atomic correctness Fix any $\kappa, N \in \mathbb{N}$, any $(\mathsf{mk}, \{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta}) \leftarrow \mathsf{Setup\text{-}at}(1^\kappa, N)$, any $\mathcal{S} \subseteq \mathcal{ID}$ such that $|\mathcal{S}| \leq N$, any $\mathsf{m} \in \mathcal{M}$, any $\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma_{\mathsf{id}}} \leftarrow \mathsf{Join\text{-}at}(\mathsf{mk}, \mathsf{id})$, any $\mathsf{r} \xleftarrow{\mathsf{U}} \mathcal{R}$. Let $\mathsf{ct}_{\mathcal{S}} \leftarrow \mathsf{Enc}(\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta}, \mathsf{m}, \mathcal{S}; \mathsf{r})$. Then, there exists some $\Delta' \subseteq \Delta$ for every $\mathsf{id} \in \mathcal{S}$, such that $\mathsf{ct}_{\mathcal{S},\mathsf{id}} \leftarrow \mathsf{Enc\text{-}at}(\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta'}, \mathsf{id}, \mathsf{m}, \mathcal{S}; \mathsf{r})$ and $\mathsf{ct}_{\mathcal{S},\mathsf{id}} \in \mathsf{ct}_{\mathcal{S}}$. Moreover, the following conditions hold with overwhelming probability:

- $\mathsf{Dec}(\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma_{\mathsf{id}}}, \mathsf{ct}_{\mathcal{S}}) \to \mathsf{m}$.
- $\mathsf{Dec\text{-}at}(\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma'_{\mathsf{id}}}, \mathsf{ct}_{\mathcal{S},\mathsf{id}}) \to \mathsf{m}$ for some $\Gamma'_{\mathsf{id}} \subseteq \Gamma_{\mathsf{id}}$.

Namely, the above guarantees that (1) a BE ciphertext for $\mathcal{S}$ contains AtBE ciphertexts for all $\mathsf{id} \in \mathcal{S}$; (2) the BE ciphertext can be correctly decrypted by the Dec, which implies Correctness of BE; and (3) every AtBE ciphertext can be correctly decrypted by the Dec-at. Therefore, Atomic Correctness of AtBE includes Correctness of BE. Thus, we can say that a BE scheme is called an AtBE scheme if the Enc and Dec includes the Enc-at and Dec-at (satisfying the above Atomic Correctness), respectively.

3.2 Properties in existing BE schemes

As described in Sect. 1.2, Kiayias and Samari [20] assumed a special property for Anonymous BE schemes in their analysis, and it is difficult to check whether the property holds for existing Anonymous BE schemes. Therefore, our goal is to replace that property with a natural one that could be checked if it holds for existing Anonymous BE schemes. In order to achieve this, we describe four properties that holds in most of existing (i.e., both non-Anonymous and Anonymous) BE schemes in this section. In particular, we show that they hold for the pairing-based BE scheme of Boneh et al. [5]. The four properties are described as follows:

Property 1 When a ciphertext has intended recipient set $\mathcal{S}$, then any recipient in $\mathcal{S}$ can obtain the underlying message by decrypting at least one of the corresponding atomic ciphertexts. More formally, ciphertext $\mathsf{ct}_{\mathcal{S}}$ output from the Enc algorithm consists of the atomic ciphertexts $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$ obtained by the $\mathsf{Enc\text{-}at}$ algorithm, and other elements.[7] In other words, let a set of atomic ciphertext contained in $\mathsf{ct}_{\mathcal{S}}$ be $\{\mathsf{ct}_{\mathcal{S},\mathsf{id}}\}_{\mathsf{id}\in\mathcal{S}}$, and let the union of $\{\mathsf{ct}_{\mathcal{S},\mathsf{id}}\}_{\mathsf{id}\in\mathcal{S}}$ and other elements contained in $\mathsf{ct}_{\mathcal{S}}$ be $\{\mathsf{ct}_{\mathcal{S}}^{(\theta)}\}_{\theta\in[\beta_{\mathcal{S}}]}$, it holds that $\{\mathsf{ct}_{\mathcal{S},\mathsf{id}}\}_{\mathsf{id}\in\mathcal{S}} \subseteq \{\mathsf{ct}_{\mathcal{S}}^{(\theta)}\}_{\theta\in[\beta_{\mathcal{S}}]} \subseteq \mathsf{ct}_{\mathcal{S}}$. Here, the randomness r input to $\mathsf{Enc\text{-}at}$ is the same when generating each atomic ciphertext in $\{\mathsf{ct}_{\mathcal{S},\mathsf{id}}\}_{\mathsf{id}\in\mathcal{S}}$. Also, inside the Dec algorithm, the $\mathsf{Dec\text{-}at}$ algorithm takes an atomic ciphertext and a set of atomic decryption keys as input, and outputs a message. If $\mathsf{ct}_{\mathcal{S}}$ is a valid ciphertext, then there is an atomic ciphertext $\mathsf{ct}_{\mathcal{S}}^{(\theta)}$ in $\mathsf{ct}_{\mathcal{S}}$ that can be decrypted using a subset of atomic decryption keys of a recipient id in $\mathcal{S}$. Formally, we require the following property for AtBE $\Pi^{\mathsf{At\text{-}BE}}$:

For all $\kappa, N \in \mathbb{N}$, all $(\mathsf{mk}, \{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta}) \leftarrow \mathsf{Setup\text{-}at}(1^{\kappa}, N)$, all $\mathsf{m} \in \mathcal{M}$, all $\mathcal{S} \subseteq \mathcal{ID}$ such that $|\mathcal{S}| \leq N$, all $\mathsf{id} \in \mathcal{ID}$, all $\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma_{\mathsf{id}}} \leftarrow \mathsf{Join\text{-}at}(\mathsf{mk}, \mathsf{id})$, all $\mathsf{r} \xleftarrow{\cup} \mathcal{R}$, all $\{\mathsf{ct}_{\mathcal{S}}^{(\theta)}\}_{\theta\in[\beta_{\mathcal{S}}]} \subseteq \mathsf{ct}_{\mathcal{S}} \leftarrow \mathsf{Enc}(\{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta}, \mathsf{m}, \mathcal{S}; \mathsf{r})$, if $\mathsf{id} \in \mathcal{S}$, then for some $\Gamma'_{\mathsf{id}} \subseteq \Gamma_{\mathsf{id}}$, there exists $\theta \in [\beta_{\mathcal{S}}]$ such that $\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma'_{\mathsf{id}}}, \mathsf{ct}_{\mathcal{S}}^{(\theta)})$ with overwhelming probability. If $\mathsf{id} \notin \mathcal{S}$, then for all $\Gamma'_{\mathsf{id}} \subseteq \Gamma_{\mathsf{id}}$, there is no $\theta \in [\beta_{\mathcal{S}}]$ such that $\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma'_{\mathsf{id}}}, \mathsf{ct}_{\mathcal{S}}^{(\theta)})$ with overwhelming probability.

Property 2 A triplet of recipient, recipient set, and message $(\mathsf{id}, \mathcal{S}, \mathsf{m})$ uniquely determines the minimum subset of atomic public keys required to generate an atomic ciphertext $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$. More formally, when generating $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$ such that $\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma'_{\mathsf{id}}}, \mathsf{ct}_{\mathcal{S},\mathsf{id}})$ for some $\gamma \in \Gamma'_{\mathsf{id}}$, let $\Delta^*_{\mathsf{id},\mathcal{S},\mathsf{m}}$ be the minimum subset of atomic public keys required for input to $\mathsf{Enc\text{-}at}$. In this case, for any $\mathcal{S} \subset \mathcal{ID}$, any $\mathsf{id} \in \mathcal{S}$, and any $\mathsf{m}, \in \mathcal{M}$, $\Delta^*_{\mathsf{id},\mathcal{S},\mathsf{m}}$ is uniquely determined by pairs of $(\mathsf{id}, \mathcal{S}, \mathsf{m})$ to input to $\mathsf{Enc\text{-}at}$.

Property 3 A pair of recipient and recipient set $(\mathsf{id}, \mathcal{S})$ uniquely determines the minimum subset of atomic decryption keys required to decrypt a (correctly-generated) atomic ciphertext $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$. More formally, when $\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma'_{\mathsf{id}}}, \mathsf{ct}_{\mathcal{S},\mathsf{id}})$ holds, let $\Gamma^*_{\mathsf{id},\mathcal{S}}$ be the minimum subset of atomic decryption keys required for input to the $\mathsf{Dec\text{-}at}$. In this case, for any $\mathcal{S} \subset \mathcal{ID}$ and any $\mathsf{id} \in \mathcal{S}$, $\Gamma^*_{\mathsf{id},\mathcal{S}}$ is uniquely determined by pairs of $(\mathsf{id}, \mathcal{S})$ to input to the $\mathsf{Enc\text{-}at}$ when generating $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$.

Property 4 If two atomic ciphertexts $\mathsf{ct}_{\mathcal{S},\mathsf{id}}, \mathsf{ct}_{\mathcal{S},\mathsf{id}'}$ are identical, then the two corresponding minimum subsets of atomic public keys generating $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$ and $\mathsf{ct}_{\mathcal{S},\mathsf{id}'}$ are also identical. More formally, for all $(\mathsf{mk}, \{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta}) \leftarrow \mathsf{Setup}(1^{\kappa}, N), \mathsf{id}, \mathsf{id}' \in$

[7] The "other elements" indicate, e.g., a signature for atomic ciphertexts (found in [25])

$\mathcal{ID}$, all $\mathcal{S} \subset \mathcal{ID}$ such that $\{\mathsf{id}, \mathsf{id}'\} \subseteq \mathcal{S}$, all $\mathsf{m} \in \mathcal{M}, \mathsf{r} \in \mathcal{R}$, all $\mathsf{ct}_{\mathcal{S},\mathsf{id}} \leftarrow \mathsf{Enc\text{-}at}(\{\mathsf{pk}^{(\delta)}\}_{\delta \in \Delta^*_{\mathsf{id},\mathcal{S},\mathsf{m}}}, \mathsf{id}, \mathsf{m}, \mathcal{S}; \mathsf{r})$, $\mathsf{ct}_{\mathcal{S},\mathsf{id}'} \leftarrow \mathsf{Enc\text{-}at}(\{\mathsf{pk}^{(\delta')}\}_{\delta' \in \Delta^*_{\mathsf{id}',\mathcal{S},\mathsf{m}}}, \mathsf{id}', \mathsf{m}, \mathcal{S}; \mathsf{r})$, if $\mathsf{ct}_{\mathcal{S},\mathsf{id}} = \mathsf{ct}_{\mathcal{S},\mathsf{id}'}$ holds, then we have $\{\mathsf{pk}^{(\delta)}\}_{\delta \in \Delta^*_{\mathsf{id},\mathcal{S},\mathsf{m}}} = \{\mathsf{pk}^{(\delta')}\}_{\delta' \in \Delta^*_{\mathsf{id}',\mathcal{S},\mathsf{m}}}$ with overwhelming probability.

We show that the BE scheme in [5] meets Properties 1, 2, 3 and 4. in Appendix A. In addition, we can similarly show that the existing (both non-Anonymous and Anonymous) BE schemes [1–3, 6, 15, 16, 24, 25, 30, 38] satisfy Properties 1, 2, 3 and 4 as well, thus it is reasonable to assume Properties 1, 2, 3 and 4 in this paper.

3.3 Security definitions for AtBE

We define chosen ciphertext security and anonymity for AtBE in the same way as in BE. In the following, we give definitions of anonymity and indistinguishability against chosen ciphertext attacks for AtBE ((**Full-**)**ANOat-IND-CCA**), IND-CCA (**INDat-CCA**) and (full) anonymity ((**Full-**)**ANOat-CCA**).

Security games for AtBE are the same as those for BE except that an attacker obtains explicitly-divided public keys, decryption keys, and a challenge ciphertext. Essentially, there is no difference in the information the attacker obtains between security games for BE and those for AtBE. Therefore, we consider (Full-)ANOat-IND-CCA, INDat-CCA and (Full-)ANOat-CCA defined below to be equivalent security notions as (Full-)ANO-IND-CCA, IND-CCA and (Full-)ANO-CCA, respectively.

Chosen ciphertext security and anonymity for AtBE Let A be any PPT adversary against Full-ANOat-IND-CCA security. We define Full-ANOat-IND-CCA with an experiment $\mathsf{Exp}^{\mathsf{Full}\text{-}ANOat\text{-}\mathsf{IND\text{-}CCA}}_{\Pi^{\mathsf{At\text{-}BE}},\mathsf{A}}$ which is the same as $\mathsf{Exp}^{\mathsf{Full}\text{-}ANO\text{-}\mathsf{IND\text{-}CCA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}$ except for the following changes to key-generation query, corruption query:

- Key-generation Query: Upon a query $\mathsf{id} \in \mathcal{ID}$ from A, C adds id to $\mathcal{D}$ and generates $\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma_{\mathsf{id}}} \leftarrow \mathsf{Join\text{-}at}(\mathsf{mk}, \mathsf{id})$, not $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{Join}(\mathsf{mk}, \mathsf{id})$.
- Corruption Query: Upon a query $\mathsf{id} \in \mathcal{D}$ from A, C adds id to $\mathcal{CD}$, and returns $\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma_{\mathsf{id}}}$ to A, not $\mathsf{sk}_{\mathsf{id}}$.

We can also define ANOat-IND-CCA with an experiment $\mathsf{Exp}^{\mathsf{ANOat\text{-}IND\text{-}CCA}}_{\Pi^{\mathsf{At\text{-}BE}},\mathsf{A}}(\kappa, N)$ which is the same as $\mathsf{Exp}^{\mathsf{Full}\text{-}ANOat\text{-}\mathsf{IND\text{-}CCA}}_{\Pi^{\mathsf{At\text{-}BE}},\mathsf{A}}(\kappa, N)$ except for the following additional condition of the restriction for challenge query: $|\mathcal{S}_0| = |\mathcal{S}_1|$.

Definition 8 ((Full-)ANOat-IND-CCA) We say $\Pi^{\mathsf{At\text{-}BE}}$ is X-CCA secure (X $\in$ {Full-ANOat-IND, ANOat-IND}) secure if for any PPT adversary A, for all sufficiently-large $\kappa \in \mathbb{N}$ and all $N \in \mathbb{N}$, it holds that $\mathsf{Adv}^{X}_{\Pi^{\mathsf{At\text{-}BE}},\mathsf{A}}(\kappa, N) < \mathsf{negl}(\kappa)$, where $\mathsf{Adv}^{X}_{\Pi^{\mathsf{At\text{-}BE}},\mathsf{A}}(\kappa, N) := \left|\Pr\left[\mathsf{Exp}^{X}_{\Pi^{\mathsf{At\text{-}BE}},\mathsf{A}}(\kappa, N) \to 1\right] - \frac{1}{2}\right|$.

We also define INDat-CCA with an experiment $\mathsf{Exp}^{\mathsf{INDat\text{-}CCA}}_{\Pi^{\mathsf{At\text{-}BE}},\mathsf{A}}(\kappa, N)$ which is the same as $\mathsf{Exp}^{\mathsf{Full}\text{-}ANOat\text{-}\mathsf{IND\text{-}CCA}}_{\Pi^{\mathsf{At\text{-}BE}},\mathsf{A}}(\kappa, N)$, except for the following additional condition of the restriction for challenge query: $\mathcal{S}_0 = \mathcal{S}_1$.

Definition 9 (INDat-CCA) We say $\Pi^{\mathsf{At\text{-}BE}}$ is INDat-CCA secure secure if for any PPT adversary A, for all sufficiently-large $\kappa \in \mathbb{N}$ and all $N \in \mathbb{N}$, it holds that $\mathsf{Adv}^{\mathsf{INDat\text{-}CCA}}_{\Pi^{\mathsf{At\text{-}BE}},\mathsf{A}}(\kappa, N) < \mathsf{negl}(\kappa)$, where $\mathsf{Adv}^{\mathsf{INDat\text{-}CCA}}_{\Pi^{\mathsf{At\text{-}BE}},\mathsf{A}}(\kappa, N) := \left|\Pr\left[\mathsf{Exp}^{\mathsf{INDat\text{-}CCA}}_{\Pi^{\mathsf{At\text{-}BE}},\mathsf{A}}(\kappa, N) \to 1\right] - \frac{1}{2}\right|$.

Also, (Full-)ANOat-CCA can be defined with experiments $\mathsf{Exp}^{\text{Full-ANOat-CCA}}_{\Pi^{\text{At-BE}},\mathsf{A}}(\kappa, N)$ and $\mathsf{Exp}^{\text{ANOat-CCA}}_{\Pi^{\text{At-BE}},\mathsf{A}}(\kappa, N)$ which are the same as $\mathsf{Exp}^{\text{Full-}ANOat\text{-IND-CCA}}_{\Pi^{\text{At-BE}},\mathsf{A}}(\kappa, N)$ and $\mathsf{Exp}^{\text{ANOat-IND-CCA}}_{\Pi^{\text{At-BE}},\mathsf{A}}(\kappa, N)$ respectively, except for the following additional condition of the restriction for challenge query: $\mathsf{m}_0 = \mathsf{m}_1$.

Definition 10 ((Full-)ANOat-CCA) We say $\Pi^{\text{At-BE}}$ is X-CCA secure (X $\in$ {Full-ANOat, ANOat}) secure if for any PPT adversary A, for all sufficiently-large $\kappa \in \mathbb{N}$ and all $N \in \mathbb{N}$, it holds that $\mathsf{Adv}^{X}_{\Pi^{\text{At-BE}},\mathsf{A}}(\kappa, N) < \mathsf{negl}(\kappa)$, where $\mathsf{Adv}^{X}_{\Pi^{\text{At-BE}},\mathsf{A}}(\kappa, N) := \left|\Pr\left[\mathsf{Exp}^{X}_{\Pi^{\text{At-BE}},\mathsf{A}}(\kappa, N) \to 1\right] - \frac{1}{2}\right|$.

4 Asymptotic lower bounds in ANO-BE

We derive lower bounds for AtBE schemes with ANOat-CCA security and Full-ANOat-CCA security. First, we define a property assumed for AtBE schemes and show that it holds for the ANO-BE scheme of Libert et al. [25]. Then, we derive lower bounds ANO-BE and Full-ANO-BE with the property described in Sect. 4.1. In the following analysis, we assume that an AtBE scheme satisfies INDat-CCA security, although this is not explicitly stated.

4.1 A property of ANO-BE and Full-ANO-BE

In order to derive lower bounds for ANO-BE and Full-ANO-BE, we assume a property that "a minimum subset of atomic decryption keys used to decrypt ciphertexts is uniquely determined by a subset of public keys used to generate the ciphertext." Specifically, we consider the following property for both ANO-BE and Full-ANO-BE (See Sect. 1.2 for the intuitive definition.):

Assumption 2 When $(\mathsf{mk}, \{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta}) \leftarrow \mathsf{Setup}(1^\kappa, N)$ is generated, we denote $\mathcal{PK}^*$ as a set of all atomic public keys, namely $\mathcal{PK}^* := \{\mathsf{pk}^{(\delta)}\}_{\delta\in\Delta}$. And, when $\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma_{\mathsf{id}}} \leftarrow \mathsf{Join\text{-}at}(\mathsf{mk}, \mathsf{id})$ is generated, $\mathcal{SK}^*$ denotes a family of the minimum subsets of atomic decryption keys to be input to the $\mathsf{Dec\text{-}at}$, namely $\mathcal{SK}^* := \{\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma^*_{\mathsf{id},\mathcal{S}}}\}_{\mathsf{id}\in\mathcal{ID},\mathcal{S}\subseteq\mathcal{ID}}$. Here, we note that $\mathcal{SK}^*$ is uniquely determined, since $\mathsf{Join\text{-}at}$ is a deterministic algorithm. At this time, for all $\mathsf{id} \in \mathcal{ID}$, all $\mathcal{S} \subseteq \mathcal{ID}$, all $\mathsf{m} \in \mathcal{M}$, all $\mathsf{r} \in \mathcal{R}$, all $\mathsf{pk}' \in 2^{\mathcal{PK}^*}$, all $\mathsf{ct}_{\mathcal{S},\mathsf{id}} \leftarrow \mathsf{Enc\text{-}at}(\mathsf{pk}', \mathsf{id}, \mathsf{m}, \mathcal{S}; \mathsf{r})$, a set of atomic decryption keys $\mathsf{sk}' \in \mathcal{SK}^* \cup \{\perp\}$ such that $\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\mathsf{sk}', \mathsf{ct}_{\mathcal{S},\mathsf{id}})$ is uniquely determined by the set of atomic public keys pk'.

ANO-BE schemes satisfying the above property include Libert et al.'s scheme [25], which is a generic construction using a public key encryption PKE and one-time signature OTS. We show that the scheme in [25] meets the property in Appendix A.

In addition, we can similarly show that all of the existing ANO-BE and Full-ANO-BE schemes in [3, 20, 24, 25] satisfy Assumption 2.

4.2 Lower bounds in ANOat-CCA secure AtBE

First, we show two lemmas, Lemma 2 and 3, for an ANOat-CCA secure AtBE with Properties 1, 2, 3 and 4 described in Sect. 3.2. In Lemma 2, we show that "if an AtBE is ANOat-CCA secure, then for ciphertexts with a set $\mathcal{S}_0, \mathcal{S}_1$ whose size is equal, sets of atomic decryption keys used by a receipient id for each decryption is identical with overwhelming probability." Then, in Lemma 3, we show that "if an AtBE is ANOat-CCA secure, then for any set $\mathcal{S}$ with

more than two elements, recipients $\mathsf{id}, \mathsf{id}' \in \mathcal{S}$ must not share a set of atomic decryption keys used to decrypt $\mathsf{ct}_{\mathcal{S}}$ with overwhelming probability."

Then, for an ANOat-CCA secure AtBE with the property described in Assumption 2, we will derive a lower bound on ciphertext-size by Theorem 1.

For convenience, for any $\mathcal{S}_0, \mathcal{S}_1 \subseteq \mathcal{ID}$, we call $(\mathcal{S}_0, \mathcal{S}_1)$ *challengeable sets* if it can be used for a challenge query in the ANOat-CCA game $\mathsf{Exp}^{\mathsf{ANOat\text{-}CCA}}_{\Pi^{\mathsf{At\text{-}BE}},\mathsf{A}}$.

Lemma 2 *If AtBE* $\Pi^{\mathsf{At\text{-}BE}}$ *is ANOat-CCA secure, no PPT adversary* A *in the ANOat-CCA game can find* $\mathsf{id} \in \mathcal{ID}$ *and challengable sets* $(\mathcal{S}_0, \mathcal{S}_1) \in \left(2^{\mathcal{D}}_{\leq N}\right)^2$ *such that* $\mathsf{id} \in \mathcal{S}_0 \cap \mathcal{S}_1$, $|\mathcal{S}_0| = |\mathcal{S}_1|$, *and* $\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}_0}} \neq \{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}_1}}$ *with non-negligible probability.*

Proof We show this lemma by contraposition. Suppose that there exists a PPT adversary A that can find $(\mathsf{id}, \mathcal{S}_0, \mathcal{S}_1)$ in the ANOat-CCA game such that $(\mathcal{S}_0, \mathcal{S}_1)$ is challengeable sets and it holds that $\mathsf{id} \in \mathcal{S}_0 \cap \mathcal{S}_1$, $|\mathcal{S}_0| = |\mathcal{S}_1|$, and $\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}_0}} \neq \{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}_1}}$ with non-negligible probability. Note that by Property 3, $\Gamma^*_{\mathsf{id},\mathcal{S}_0}$ and $\Gamma^*_{\mathsf{id},\mathcal{S}_1}$ are uniquely determined. Then, A can break ANOat-CCA security as follows. During the ANOat-CCA game, A can find $(\mathsf{id}^*, \mathcal{S}_0, \mathcal{S}_1)$ such that $\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}^*}\}_{\gamma \in \Gamma^*_{\mathsf{id}^*,\mathcal{S}_0}} \neq \{\mathsf{sk}^{(\gamma)}_{\mathsf{id}^*}\}_{\gamma \in \Gamma^*_{\mathsf{id}^*,\mathcal{S}_1}}$. A then issues key-generation queries for every $\mathsf{id} \in \mathcal{S}_0 \cup \mathcal{S}_1$ and a corruption query for id^* (if A has not done them yet), and obtains a decryption key $\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}^*}\}_{\gamma \in \Gamma_{\mathsf{id}^*}}$. A then issues a challenge query $(\mathsf{m}, \mathcal{S}_0, \mathcal{S}_1)$ to obtain $\{\mathsf{ct}^{(\theta)}_{\mathcal{S}_b}\}_{\theta \in [\beta_{\mathcal{S}_b}]} \subseteq \mathsf{ct}_{\mathcal{S}_b}$. Note that A can get the decryption key for id^* since $\mathsf{id}^* \in \mathcal{S}_0 \cap \mathcal{S}_1$ and $(\mathcal{S}_0, \mathcal{S}_1)$ can be used for the challenge query. Finally, A outputs $b' = 0$ if there exists $\theta \in [\beta_{\mathcal{S}_b}]$ such that $\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}^*}\}_{\gamma \in \Gamma^*_{\mathsf{id}^*,\mathcal{S}_0}}, \mathsf{ct}^{(\theta)}_{\mathcal{S}_b})$, and $b' = 1$ otherwise. In this case, A can output b' such that $b = b'$ with non-negligible probability. □

Lemma 3 *If AtBE* $\Pi^{\mathsf{At\text{-}BE}}$ *is ANOat-CCA secure, no PPT adversary* A *in the ANOat-CCA game can find* $(\mathsf{id}, \mathsf{id}', \mathcal{S}) \in \mathcal{ID}^2 \times 2^{\mathcal{D}}_{\leq N}$ *such that* $\mathsf{id}, \mathsf{id}' \in \mathcal{S}$ *and* $\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{id,\mathcal{S}}} \neq \{\mathsf{sk}^{(\gamma')}_{\mathsf{id}'}\}_{\gamma' \in \Gamma^*_{\mathsf{id}',\mathcal{S}}}$ *with non-negligible probability.*

Proof Assume on the contrary that there exists a PPT adversary A that can find $(\mathsf{id}, \mathsf{id}', \mathcal{S})$ such that $\mathsf{id}, \mathsf{id}' \in \mathcal{S}$ and $\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}}} = \{\mathsf{sk}^{(\gamma')}_{\mathsf{id}'}\}_{\gamma' \in \Gamma^*_{\mathsf{id}',\mathcal{S}}}$ with non-negligible probability. Note that by Property 3, $\Gamma^*_{\mathsf{id},\mathcal{S}}$ and $\Gamma^*_{\mathsf{id}',\mathcal{S}}$ are uniquely determined. Then, we will show that it contradicts Property 1 of AtBE in Sect. 3.2 for any $\mathcal{S}'$ such that $\mathsf{id} \in \mathcal{S}'$, $\mathsf{id}' \notin \mathcal{S}'$, and $|\mathcal{S}| = |\mathcal{S}'|$. Suppose that A has atomic decryption keys $\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma_{\mathsf{id}}}$ and $\{\mathsf{sk}^{(\gamma')}_{\mathsf{id}'}\}_{\gamma' \in \Gamma_{\mathsf{id}'}}$ by key-generation queries and corruption queries. Since $\mathsf{id} \in \mathcal{S}'$, we have $\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}'}}, \mathsf{ct}_{\mathcal{S}',\mathsf{id}})$. From Lemma 2, we have $\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}'}} = \{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}}}$ with overwhelming probability.[8]

Hence, we have $\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}}}, \mathsf{ct}_{\mathcal{S}',\mathsf{id}})$. Here, since $\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}}} = \{\mathsf{sk}^{(\gamma')}_{\mathsf{id}'}\}_{\gamma' \in \Gamma^*_{\mathsf{id}',\mathcal{S}}}$ from the assumption, we have $\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}^{(\gamma')}_{\mathsf{id}'}\}_{\gamma' \in \Gamma^*_{\mathsf{id}',\mathcal{S}}}, \mathsf{ct}_{\mathcal{S}',\mathsf{id}})$. However, since $\mathsf{id}' \notin \mathcal{S}'$ holds, the above contradicts Property 1. □

In the following, we derive a lower bound on ciphertext-size in ANOat-CCA secure AtBE with the property described in Assumption 2. Specifically, we show the statement: When there exists a set $\mathcal{S}$ such that the number of atomic ciphertexts $\mathsf{ct}_{\mathcal{S}}$ contained in $\mathsf{ct}_{\mathcal{S}}$ is less than $|\mathcal{S}|$ with non-negligible probability, a contradiction occurs for Lemma 3.

[8] Otherwise, A can find $(\mathsf{id}, \mathcal{S}_0, \mathcal{S}_1)$ which contradicts Lemma 2.

Theorem 1 *If AtBE* $\Pi^{\mathsf{At\text{-}BE}}$ *is ANOat-CCA secure and has the property in Assumption 2, the size of ciphertexts for any recipient set* $\mathcal{S} \in 2^{\mathcal{ID}}_{\leq N}$ *and any message* $\mathsf{m} \in \mathcal{M}$ *is* $\Omega(|\mathcal{S}| \cdot k)$ *with overwhelming probability, where* $k = \min_{\mathcal{S} \subseteq \mathcal{ID}, \theta \in [\beta_{\mathcal{S}}]} |\mathsf{ct}^{(\theta)}_{\mathcal{S}}|$ *and the probability is taken over the internal randomness of the* Setup-at, Enc, *and* Enc-at. *In other words, if AtBE* $\Pi^{\mathsf{At\text{-}BE}}$ *is ANOat-CCA secure and has the property in Assumption 2, for any recipient set* $\mathcal{S} \in 2^{\mathcal{ID}}_{\leq N}$ *and any message* $\mathsf{m} \in \mathcal{M}$*, the* Enc *outputs a ciphertext of size* $\Omega(|\mathcal{S}| \cdot k)$ *with overwhelming probability.*

Proof For some set of recipients $\mathcal{S}^* \in 2^{\mathcal{ID}}_{\leq N}$ and message $\mathsf{m}^* \in \mathcal{M}$, we assume that with non-negligible probability, the Enc outputs $\mathsf{ct}_{\mathcal{S}^*} = \{\mathsf{ct}^{(\theta)}_{\mathcal{S}^*}\}_{\theta \in [\beta_{\mathcal{S}^*}]} \leftarrow \mathsf{Enc}(\{\mathsf{pk}^{(\delta)}\}_{\delta \in \Delta}, \mathsf{m}^*, \mathcal{S}^*; \mathsf{r}^*)$ and $\beta_{\mathcal{S}^*} < |\mathcal{S}^*|$. Let A be any fixed PPT adversary against the ANOat-CCA game. Then, A can identify such $(\mathcal{S}^*, \mathsf{m}^*)$ with non-negligible probability since A knows the concrete procedure of the Enc (since it should be public due to Kerckhoffs' principle).[9] We then show that A can find $(\mathsf{id}, \mathsf{id}', \mathcal{S}^*)$ that contradicts Lemma 3. Now, from $\beta_{\mathcal{S}^*} \geq 1$, we consider that $|\mathcal{S}^*| \geq 2$ holds. From $\beta_{\mathcal{S}^*} < |\mathcal{S}^*|$, for a set of atomic ciphertexts $\{\mathsf{ct}^{(\theta)}_{\mathcal{S}^*}\}_{\theta \in \beta_{\mathcal{S}^*}}$, there exists at least one atomic ciphertext $\mathsf{ct}^{(\theta^*)}_{\mathcal{S}^*}$ that can be decrypted by two recipients $\mathsf{id}, \mathsf{id}' \in \mathcal{S}^*$. That is, for $\mathsf{id}, \mathsf{id}' \in \mathcal{S}^*$, it holds that $\mathsf{ct}^{(\theta^*)}_{\mathcal{S}^*} = \mathsf{ct}_{\mathcal{S},\mathsf{id}} = \mathsf{ct}_{\mathcal{S},\mathsf{id}'}$, where $\mathsf{ct}_{\mathcal{S},\mathsf{id}}, \mathsf{ct}_{\mathcal{S},\mathsf{id}'}$ is generated by

$$\mathsf{ct}_{\mathcal{S},\mathsf{id}} \leftarrow \mathsf{Enc\text{-}at}(\{\mathsf{pk}^{(\delta)}\}_{\delta \in \Delta^*_{\mathsf{id},\mathcal{S}^*,\mathsf{m}^*}}, \mathsf{id}, \mathsf{m}^*, \mathcal{S}^*; \mathsf{r}^*),$$
$$\mathsf{ct}_{\mathcal{S},\mathsf{id}'} \leftarrow \mathsf{Enc\text{-}at}(\{\mathsf{pk}^{(\delta)}\}_{\delta \in \Delta^*_{\mathsf{id}',\mathcal{S}^*,\mathsf{m}^*}}, \mathsf{id}', \mathsf{m}^*, \mathcal{S}^*; \mathsf{r}^*),$$

where r^* is the same randomness in the Enc above. Note that by Property 2, $\Delta^*_{\mathsf{id},\mathcal{S}^*,\mathsf{m}^*}$ and $\Delta^*_{\mathsf{id}',\mathcal{S}^*,\mathsf{m}^*}$ are uniquely determined, and by Property 4, it holds $\{\mathsf{pk}^{(\delta)}\}_{\delta \in \Delta^*_{\mathsf{id},\mathcal{S}^*,\mathsf{m}^*}} = \{\mathsf{pk}^{(\delta)}\}_{\delta \in \Delta^*_{\mathsf{id}',\mathcal{S}^*,\mathsf{m}^*}}$. In addition, by Atomic Correctness and Property 1, we have

$$\mathsf{m}^* \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}^*}}, \mathsf{ct}^{(\theta^*)}_{\mathcal{S}^*}),$$
$$\mathsf{m}^* \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}^{(\gamma')}_{\mathsf{id}'}\}_{\gamma' \in \Gamma^*_{\mathsf{id}',\mathcal{S}^*}}, \mathsf{ct}^{(\theta^*)}_{\mathcal{S}^*}).$$

Note that by Property 3, $\{\mathsf{sk}^{(\gamma')}_{\mathsf{id}'}\}_{\gamma' \in \Gamma^*_{\mathsf{id},\mathcal{S}^*}}$ and $\{\mathsf{sk}^{(\gamma')}_{\mathsf{id}'}\}_{\gamma' \in \Gamma^*_{\mathsf{id}',\mathcal{S}^*}}$ are uniquely determined. From Assumption 2, $\{\mathsf{pk}^{(\delta)}\}_{\delta \in \Delta^*_{\mathsf{id},\mathcal{S}^*,\mathsf{m}^*}}$ and $\{\mathsf{pk}^{(\delta)}\}_{\delta \in \Delta^*_{\mathsf{id}',\mathcal{S}^*,\mathsf{m}^*}}$ uniquely determine $\{\mathsf{sk}^{(\gamma')}_{\mathsf{id}}\}_{\gamma' \in \Gamma^*_{\mathsf{id},\mathcal{S}^*}}$ and $\{\mathsf{sk}^{(\gamma')}_{\mathsf{id}'}\}_{\gamma' \in \Gamma^*_{\mathsf{id}',\mathcal{S}^*}}$ such that

$$\mathsf{m}^* \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}^*}}, \mathsf{Enc\text{-}at}(\{\mathsf{pk}^{(\delta)}\}_{\delta \in \Delta^*_{\mathsf{id},\mathcal{S}^*,\mathsf{m}^*}}, \mathsf{id}, \mathsf{m}^*, \mathcal{S}^*; \mathsf{r}^*)),$$
$$\mathsf{m}^* \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}'}\}_{\gamma \in \Gamma^*_{\mathsf{id}',\mathcal{S}^*}}, \mathsf{Enc\text{-}at}(\{\mathsf{pk}^{(\delta)}\}_{\delta \in \Delta^*_{\mathsf{id}',\mathcal{S}^*,\mathsf{m}^*}}, \mathsf{id}', \mathsf{m}^*, \mathcal{S}^*; \mathsf{r}^*)),$$

respectively. As mentioned above, it holds $\{\mathsf{pk}^{(\delta)}\}_{\delta \in \Delta^*_{\mathsf{id},\mathcal{S}^*,\mathsf{m}^*}} = \{\mathsf{pk}^{(\delta)}\}_{\delta \in \Delta^*_{\mathsf{id}',\mathcal{S}^*,\mathsf{m}^*}}$. Therefore, despite ANOat-CCA security of $\Pi^{\mathsf{At\text{-}BE}}$, A can obtain $\{\mathsf{sk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}^*}} = \{\mathsf{sk}^{(\gamma')}_{\mathsf{id}'}\}_{\gamma' \in \Gamma^*_{\mathsf{id}',\mathcal{S}^*}}$, which contradicts Lemma 3. □

[9] From the descriptions of the Enc, A can extract the conditions for obtaining $\mathsf{ct}_{\mathcal{S}^*} = \{\mathsf{ct}^{(\theta)}_{\mathcal{S}^*}\}_{\theta \in [\beta_{\mathcal{S}^*}]}$ such that $\beta_{\mathcal{S}^*} < |\mathcal{S}^*|$ with non-negligible probability (even if $\beta_{\mathcal{S}^*}$ is determined randomly) since the Enc is a PPT algorithm. Note that A does not need to know the concrete randomness r^* to be used to compute $\mathsf{ct}_{\mathcal{S}^*}$, though A seems to need to know how the randomness is used in the Enc.

4.3 Lower bounds in Full-ANOat-CCA secure AtBE

We derive a lower bound on ciphertext size in Theorem 2 for Full-ANOat-CCA secure AtBE with the property described in Assumption 2, using Theorem 1.

Theorem 2 *If AtBE* $\Pi^{\mathsf{At\text{-}BE}}$ *is Full-ANOat-CCA secure and has the property in Assumption 2, the size of ciphertexts for any recipient set* $\mathcal{S} \in 2^{\mathcal{ID}}_{\leq N}$ *and any message* $\mathsf{m} \in \mathcal{M}$ *is* $\Omega(N \cdot k)$ *with overwhelming probability, where* $k = \min_{\mathcal{S} \subseteq \mathcal{ID}, \theta \in [\beta_{\mathcal{S}}]} |\mathsf{ct}_{\mathcal{S}}^{(\theta)}|$ *and the probability is taken over the internal randomness of the* Setup-at, Enc, *and* Enc-at. *In other words, if AtBE* $\Pi^{\mathsf{At\text{-}BE}}$ *is Full-ANOat-CCA secure and has the property in Assumption 2, for any recipient set* $\mathcal{S} \in 2^{\mathcal{ID}}_{\leq N}$ *and any message* $\mathsf{m} \in \mathcal{M}$*, the* Enc *outputs a ciphertext of size* $\Omega(N \cdot k)$ *with overwhelming probability.*

Proof Since Full-ANOat-CCA security implies ANOat-CCA security, for any $\mathcal{S} \in 2^{\mathcal{ID}}_{\leq N}$, we at least have $\Omega(|\mathcal{S}| \cdot \kappa)$ with overwhelming probability from Theorem 1. Now, we assume that for some set of recipients $\mathcal{S}^* \in 2^{\mathcal{ID}}_{\leq N}$ and message $\mathsf{m}^* \in \mathcal{M}$, Enc outputs $\mathsf{ct}_{\mathcal{S}^*} = \{\mathsf{ct}^{(\theta)}_{\mathcal{S}^*}\}_{\theta \in [\beta_{\mathcal{S}^*}]} \leftarrow \mathsf{Enc}(\{\mathsf{pk}^{(\delta)}\}_{\delta \in \Delta}, \mathsf{m}^*, \mathcal{S}^*; \mathsf{r}^*)$ such that $|\mathcal{S}^*| \leq \beta_{\mathcal{S}^*} < N$, with non-negligible probability. Let A be any fixed PPT adversary against the Full-ANOat-CCA game. Then, A can identify such $(\mathcal{S}^*, \mathsf{m}^*)$ with non-negligible probability since A knows the concrete procedure of Enc (since it should be public due to Kerckhoffs' principle). A then issues a challenge query $(\mathsf{m}^*, \mathcal{S}^*, \mathcal{S})$, where $\mathcal{S} = [N]$ and $\mathcal{S}^*$ is any set in $2^{\mathcal{ID}}_{\leq N} \setminus [N]$. Here, from the assumption that $|\mathcal{S}^*| \leq \beta_{\mathcal{S}^*} < N$, A can trivially break Full-ANOat-CCA, but it contradicts the premise. Thus, the size of ciphertexts for any $\mathcal{S} \in 2^{\mathcal{ID}}_{\leq N}$ must be equal to that of ciphertexts for $[N]$ at least, i.e., $\Omega(N \cdot \kappa)$. □

5 Non-asymptotic bounds and optimal constructions of ANO-BE

We show (non-asymptotic) upper bounds and lower bounds on the ciphertext-size in ANO-BE. Li and Gong [24] proposed an ANO-BE scheme where the ciphertext-size is $(|\mathcal{S}|+6)\cdot\kappa$, which is indeed *optimal* in the sense that the scheme attains the lower bound on the ciphertext size (i.e., Theorem 1) non-asymptotically (see Theorem 5). On the other hand, there exists no optimal Full-ANO-BE scheme. To show a non-asymptotic upper bound on the ciphertext-size in Full-ANO-BE, we propose an optimal Full-ANO-BE scheme.

Our scheme is achieved by modifying the encryption algorithm Enc and the decryption algorithm Dec in Li and Gong [24]'s ANO-BE.

- $\mathsf{Setup}(1^\kappa, N)$: Run $\mathsf{PGGen}(1^\kappa)$ to get $\mathcal{PG} := (\mathsf{p}, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, \mathsf{g}_1, \mathsf{g}_2)$. Let $\mathbf{A}, \mathbf{B} \xleftarrow{\mathsf{U}} \mathcal{D}_k$ and $\mathbf{X}, \mathbf{Y} \xleftarrow{\mathsf{U}} \mathbb{Z}_p^{(k+1)\times(k+1)}$. For all $\mathsf{id} \in [N]$, sample $\mathbf{k}_{\mathsf{id}} \xleftarrow{\mathsf{U}} \mathbb{Z}_p^{(k+1)}$.
  Select a key-binding secure symmetric encryption scheme $\Pi^{\mathsf{SKE}} = (\mathsf{E}, \mathsf{D})$ with the key space $\mathcal{K} := \mathbb{G}_1$. Sample a collision-resilient hash function $\mathsf{H} : \{0,1\}^* \to \mathbb{Z}_p$ from $\mathcal{H}$ uniformly at random. The public key pk is
  $$\left(\mathcal{PG}, (\mathsf{E}, \mathsf{D}), \mathsf{H}; \begin{matrix}[\mathbf{A}^\top]_1, \{[\mathbf{A}^\top \mathbf{k}_{\mathsf{id}}]_1\}_{\mathsf{id}=1}^N, [\mathbf{B}]_2, \\ [\mathbf{A}^\top \mathbf{Y}]_1, [\mathbf{A}^\top \mathbf{X}]_1, [\mathbf{X}\mathbf{B}]_2, [\mathbf{Y}\mathbf{B}]_2\end{matrix}\right).$$
  and the master secret key is $\{\mathbf{k}_{\mathsf{id}}\}_{\mathsf{id}=1}^N$.
- $\mathsf{Join}(\mathsf{mk}, \mathsf{id})$: Output the secret key $\mathsf{sk}_{\mathsf{id}} := \mathbf{k}_{\mathsf{id}}$.

- $\mathsf{Enc}(\mathsf{pk}, \mathsf{m}, \mathcal{S})$: Let n be the number of recipients currently participating in the system, and suppose that $\mathsf{sk}_{\mathsf{id}_1}, \ldots, \mathsf{sk}_{\mathsf{id}_n}$ have been generated by the Join so far. Sample $\mathbf{r} \xleftarrow{\cup} \mathbb{Z}_p^k$, and compute $\left[\mathbf{u}^\top\right] := \left[\mathbf{r}^\top \mathbf{A}^\top\right]$. Select a session key $\mathsf{K} \xleftarrow{\cup} \mathbb{G}_1$ and compute $\mathsf{c}_0 := \mathsf{E}_{\mathsf{K}}(\mathsf{m})$. Compute the following for all $\mathsf{id} \in [N]$:

$$\begin{cases} \mathsf{c}_{\mathsf{id}} := \left[\mathbf{r}^\top \mathbf{A}^\top \mathbf{k}_{\mathsf{id}}\right]_1 \cdot \mathsf{K}, \text{ if } \mathsf{id} \in \mathcal{S}, \\ \mathsf{c}_{\mathsf{id}} \xleftarrow{\cup} \mathbb{G}_1, \text{ if } \mathsf{id} \notin \mathcal{S}. \end{cases} \tag{1}$$

  Choose a random permutation σ from $\{\sigma_i : [N] \to [N]\}_{i \in \{0,1\}^\kappa}$ and compute $[\boldsymbol{\pi}]_1 := \left[\mathbf{r}^\top \mathbf{A}^\top (\mathbf{X} + \alpha \cdot \mathbf{Y})\right]_1$ where $\alpha := \mathsf{H}(\left[\mathbf{u}^\top\right], \mathsf{c}_0, \mathsf{c}_{\sigma(1)}, \ldots, \mathsf{c}_{\sigma(N)})$. The ciphertext is

$$\mathsf{ct}_{\mathcal{S}} := (\left[\mathbf{u}^\top\right], \mathsf{c}_0, \mathsf{c}_{\sigma(1)}, \ldots, \mathsf{c}_{\sigma(N)}, [\boldsymbol{\pi}]_1).$$

  Here, in the scheme of [24], only c_{id} $(\mathsf{id} \in \mathcal{S})$ is calculated in the Eq. (1), and the following ciphertext is output.

$$\mathsf{ct}_{\mathcal{S}} := (\left[\mathbf{u}^\top\right], \mathsf{c}_0, \mathsf{c}_{\sigma(1)}, \ldots, \mathsf{c}_{\sigma(|\mathcal{S}|)}, [\boldsymbol{\pi}]_1).$$

- $\mathsf{Dec}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct}_{\mathcal{S}})$: Let $\mathsf{sk}_{\mathsf{id}} = \mathbf{k}_{\mathsf{id}}, \mathsf{ct}_{\mathcal{S}} = (\left[\mathbf{u}^\top\right], \mathsf{c}_0, \mathsf{c}_1, \ldots, \mathsf{c}_N, [\boldsymbol{\pi}]_1)$. Compute $\alpha := \mathsf{H}(\left[\mathbf{u}^\top\right], \mathsf{c}_0, \mathsf{c}_1, \ldots, \mathsf{c}_N)$ and check

$$e([\boldsymbol{\pi}]_1, [\mathbf{B}]_2) = e(\left[\mathbf{u}^\top\right]_1, [(\mathbf{X} + \alpha \cdot \mathbf{Y})\mathbf{B}]_2). \tag{2}$$

  If the above equation does not hold, return $\perp$; otherwise, do the following two steps from $j := 1$.

  - Compute $\mathsf{K}' := \mathsf{c}_j / \left[\mathbf{u}^\top \mathbf{k}_{\mathsf{id}}\right]_1$ and $\mathsf{m}' := \mathsf{D}_{\mathsf{K}'}(\mathsf{c}_0)$. If $\mathsf{m}' \neq \perp$, return m' and halt; otherwise, go to the second step.
  - If $j = N$, return $\perp$ and halt; otherwise, do the first step with $j := j + 1$.

  Here, in the scheme of [24], parse $\mathsf{ct}_{\mathcal{S}} = (\left[\mathbf{u}^\top\right], \mathsf{c}_0, \mathsf{c}_1, \ldots, \mathsf{c}_{|\mathcal{S}|}, [\boldsymbol{\pi}]_1)$, compute $\alpha := \mathsf{H}(\left[\mathbf{u}^\top\right], \mathsf{c}_0, \mathsf{c}_1, \ldots, \mathsf{c}_{|\mathcal{S}|})$, and check whether the equation (2) holds. Also, the second step above is described as follows.

  - If $j = |\mathcal{S}|$, return $\perp$ and halt; otherwise, do the first step with $j := j + 1$.

We show the correctness of the above Full-ANO-BE scheme. Suppose that $\mathsf{ct}_{\mathcal{S}} = (\left[\mathbf{u}^\top\right], \mathsf{c}_0, \mathsf{c}_1, \ldots, \mathsf{c}_N, [\boldsymbol{\pi}]_1)$, $\mathsf{sk}_{\mathsf{id}} = \mathbf{k}_{\mathsf{id}} (\mathsf{id} \in \mathcal{S})$ are correctly generated. Then the following equation holds:

$$e([\boldsymbol{\pi}]_1, [\mathbf{B}]_2) = e(\left[\mathbf{u}^\top\right]_1, [(\mathbf{X} + \alpha \cdot \mathbf{Y})\mathbf{B}]_2),$$

where $\alpha := \mathsf{H}(\left[\mathbf{u}^\top\right], \mathsf{c}_0, \mathsf{c}_1, \ldots, \mathsf{c}_N)$. Given $\mathsf{c}_j := \left[\mathbf{r}^\top \mathbf{A}^\top \mathbf{k}_{\mathsf{id}}\right]_1 \cdot \mathsf{K}$, we have $\mathsf{K} = \mathsf{c}_j / \left[\mathbf{u}^\top \mathbf{k}_{\mathsf{id}}\right]_1$ and and the Dec will return m by the correctness of symmetric encryption scheme $\Pi^{\mathsf{SKE}} = (\mathsf{E}, \mathsf{D})$. Given $\mathsf{c}_j := \left[\mathbf{r}^\top \mathbf{A}^\top \mathbf{k}_{\mathsf{id}}\right]_1 \cdot \mathsf{K}$, we have $\mathsf{K} \neq \mathsf{c}_j / \left[\mathbf{u}^\top \mathbf{k}_{\mathsf{id}'}\right]_1$ for some $\mathsf{id}' \notin \mathcal{S}$ with overwhelming probability, and the Dec will return $\perp$ from key-binding of $\Pi^{\mathsf{SKE}} = (\mathsf{E}, \mathsf{D})$.

Theorem 3 *The construction described above is Full-ANO-IND-CCA secure assuming that: (1) $\mathcal{H}$ is collision-resistant; (2) the $\mathcal{D}_k$-MDDH assumption holds in $\mathbb{G}_1$; (3) the $\mathcal{D}_k$-KerMDH assumptions holds in $\mathbb{G}_2$; (4) Π^{SKE} is semantically secure and key-binding.*

Our security proof is the same as that of Li and Gong [24]'s ANO-BE except that we added $\mathsf{c}_{\mathsf{id}} \xleftarrow{\mathsf{U}} \mathbb{G}_1$ (if $\mathsf{id} \notin \mathcal{S}$) to their scheme. We prove Full-ANO-IND-CCA security by defining the following games:

$\mathsf{Game}_{\mathsf{Real}}$: This is the same as the Full-ANO-IND-CCA game.

Game_0: This is the same as $\mathsf{Game}_{\mathsf{Real}}$ except that the challenger samples $\mathbf{u}^* \xleftarrow{\mathsf{U}} \mathbb{Z}_p^{(k+1)}$ and generates the challenge ciphertext $\mathsf{ct}^*_{\mathcal{S}} := (\left[\mathbf{u}^{*\top}\right], \mathsf{c}^*_0, \mathsf{c}^*_{\sigma(1)}, \ldots, \mathsf{c}^*_{\sigma(|\mathcal{S}|)}, [\boldsymbol{\pi}]^*_1)$ using $\mathbf{u}^*$.

Game_1: This is the same as Game_0 except for the following modification: Let $(\mathsf{id}, \mathsf{ct}_{\mathcal{S}} = (\left[\mathbf{u}^\top\right], \mathsf{c}_0, \mathsf{c}_1, \ldots, \mathsf{c}_N, [\boldsymbol{\pi}]_1))$ be a decryption query, and we denote $\overline{\mathsf{ct}_{\mathcal{S}}} = (\left[\mathbf{u}^\top\right], \mathsf{c}_0, \mathsf{c}_1, \ldots, \mathsf{c}_N)$. The Decryption Oracle computes $\alpha = \mathsf{H}(\overline{\mathsf{ct}_{\mathcal{S}}})$ and returns $\perp$ if one of the following conditions hold:

(1) $\mathsf{ct}_{\mathcal{S}} = \mathsf{ct}^*_{\mathcal{S}}$,
(2) $e([\boldsymbol{\pi}]_1, [\mathbf{B}]_2) \neq e(\left[\mathbf{u}^\top\right]_1, [(\mathbf{X} + \alpha \cdot \mathbf{Y})\mathbf{B}]_2)$,
(3) $\overline{\mathsf{ct}_{\mathcal{S}}} \neq \overline{\mathsf{ct}^*_{\mathcal{S}}}$ and $\alpha = \alpha^*$,

where $\alpha^* = \mathsf{H}(\overline{\mathsf{ct}^*_{\mathcal{S}}})$.

Game_2: This is the same as Game_1 except that the condition (2) is replaced by the following one:

$$(2')\ [\boldsymbol{\pi}]_1 \neq \left[\mathbf{u}^\top(\mathbf{X} + \alpha \cdot \mathbf{Y})\right]_1.$$

$\mathsf{Game}_{2,j}$ $(1 \leq j \leq q_D)$: This is the same as Game_2 except for the following modification: Let q_D is the maximum number of decryption queries to the Decryption Oracle. Regarding the first j queries, the Decryption Oracle returns $\perp$ if (1) or (3) or

$$(2'')\ \mathbf{u} \notin \mathrm{span}(\mathbf{A})\ ||\ [\boldsymbol{\pi}]_1 \neq \left[\mathbf{u}^\top(\mathbf{X} + \alpha \cdot \mathbf{Y})\right]_1$$

holds instead of $(2')$. Here, "||" denotes the OR operation which ignores the second operand if the first one is satisfied. For the rest of queries, the Decryption Oracle returns $\perp$ if (1) or (3) or $(2')$ as in Game_2.

Let S_{Real}, S_i $(0 \leq i \leq 2)$, and $S_{2,j}$ $(0 \leq j \leq q_D)$ be the probabilities that the event $b' = b$ occurs in $\mathsf{Game}_{\mathsf{Real}}$, Game_i, and $\mathsf{Game}_{2,j}$ respectively. We have

$$\begin{aligned}\mathsf{Adv}^{\mathsf{Full\text{-}ANO\text{-}IND\text{-}CCA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N) \leq\ & |S_{\mathsf{Real}} - S_0| + |S_0 - S_1| + |S_1 - S_2| \\ & + \Sigma_{j=1}^{q_D} \left|S_{2,j-1} - S_{2,j}\right| + \left|S_{2,q_D} - \frac{1}{2}\right|.\end{aligned}$$

The rest of the proof follows from the following lemmas.

Lemma 4 $|S_{\mathsf{Real}} - S_0| \leq \mathsf{Adv}^{\mathsf{mddh}}_{\mathsf{B},\mathbb{G}_1}(\kappa)$.

Proof At the beginning, a PPT adversary B receives an instance $([\mathbf{A}]_1, T)$ of the MDDH problem. Then, B randomly selects $\mathbf{B} \xleftarrow{\mathsf{U}} \mathcal{D}_k$ and $\mathbf{X}, \mathbf{Y} \xleftarrow{\mathsf{U}} \mathbb{Z}_p^{(k+1)\times(k+1)}$. For all $\mathsf{id} \in [N]$, B samples $\mathbf{k}_{\mathsf{id}} \xleftarrow{\mathsf{U}} \mathbb{Z}_p^{(k+1)}$. B selects a key-binding secure symmetric encryption scheme $\Pi^{\mathsf{SKE}} = (\mathsf{E}, \mathsf{D})$ with the key space $\mathcal{K} := \mathbb{G}_1$ and a collision-resilient hash function $\mathsf{H} : \{0,1\}^* \to \mathbb{Z}_p$. B sends the following master public key:

$$\mathsf{pk} := \left(\mathcal{PG}, (\mathsf{E}, \mathsf{D}), \mathsf{H}; \begin{matrix}[\mathbf{A}^\top]_1, \{[\mathbf{A}^\top\mathbf{k}_{\mathsf{id}}]_1\}_{\mathsf{id}=1}^N, [\mathbf{B}]_2, \\ [\mathbf{A}^\top\mathbf{Y}]_1, [\mathbf{A}^\top\mathbf{X}]_1, [\mathbf{XB}]_2, [\mathbf{YB}]_2\end{matrix}\right).$$

Note that B knows the master secret key $\mathsf{mk} := \{\mathbf{k}_{\mathsf{id}}\}_{\mathsf{id}=1}^N$.

Key-generation Oracle and Corruption Oracle. B can simulate the oracles since it knows the master secret key.
Decryption Oracle. B can simulate the oracle for the same reason as Key-generation and Corruption Oracle.
Challenge. B receives $(\mathsf{m}_0, \mathsf{m}_1, \mathcal{S}_0, \mathcal{S}_1)$ from A. B randomly chooses $d \xleftarrow{\mathsf{U}} \{0,1\}$ and selects a session key $\mathsf{K} \xleftarrow{\mathsf{U}} \mathbb{G}_1$ and compute $\mathsf{c}_0 := \mathsf{E}_{\mathsf{K}}(\mathsf{m}_d)$. B sets $\left[\mathbf{u}^{*\top}\right] := T$ and computes the following for all $\mathsf{id} \in [N]$:

$$\begin{cases} \mathsf{c}_{\mathsf{id}} := \left[\mathbf{u}^{*\top}\mathbf{k}_{\mathsf{id}}\right]_1 \cdot \mathsf{K}, \text{ if } \mathsf{id} \in \mathcal{S}_d, \\ \mathsf{c}_{\mathsf{id}} \xleftarrow{\mathsf{U}} \mathbb{G}_1, \text{ if } \mathsf{id} \notin \mathcal{S}_d. \end{cases}$$

Then B chooses a random permutation σ from $\{\sigma_i : [N] \to [N]\}_{i \in \{0,1\}^\kappa}$ and computes $[\boldsymbol{\pi}]_1 := \left[\mathbf{u}^{*\top}(\mathbf{X} + \alpha \cdot \mathbf{Y})\right]_1$ where $\alpha := \mathsf{H}(\left[\mathbf{u}^{*\top}\right]_1, \mathsf{c}_0, \mathsf{c}_{\sigma(1)}, \ldots, \mathsf{c}_{\sigma(N)})$. B sends the following ciphertext:

$$\mathsf{ct}_{\mathcal{S}} := (\left[\mathbf{u}^{*\top}\right]_1, \mathsf{c}_0, \mathsf{c}_{\sigma(1)}, \ldots, \mathsf{c}_{\sigma(N)}, [\boldsymbol{\pi}]_1).$$

If $b = 0$, then $\mathbf{u}^* \xleftarrow{\mathsf{U}} \mathrm{span}(\mathbf{A})$. If $b = 1$, then $\mathbf{u}^* \xleftarrow{\mathsf{U}} \mathbb{Z}_p^{k+1}$. After receiving d from A, B sends $b' = 1$ to the challenger of the $\mathcal{D}_k$-MDDH problem if $d' = d$. Otherwise, B sends $b' = 0$ to the challenger. □

Lemma 5 $|S_0 - S_1| \leq \mathsf{Adv}^{\mathsf{hash}}_{\mathsf{B}}(\kappa)$. (*From Difference Lemma* [36])

Proof By the collision-resilience of $\mathcal{H}$, Game_1 is indistinguishable from Game_0. When A issues a decryption query $(\mathsf{id}, \mathsf{ct}_{\mathcal{S}} = (\left[\mathbf{u}^\top\right], \mathsf{c}_0, \mathsf{c}_1, \ldots, \mathsf{c}_N, [\boldsymbol{\pi}]_1))$ such that $\overline{\mathsf{ct}_{\mathcal{S}}} = (\left[\mathbf{u}^\top\right], \mathsf{c}_0, \mathsf{c}_1, \ldots, \mathsf{c}_N)$ is not identical to $\overline{\mathsf{ct}^*_{\mathcal{S}}}$, B check whether the condition (3) holds. If it does not hold, then B simulates the Decryption Oracle by returning $\perp$. Otherwise, B can break the collision-resilience of $\mathcal{H}$ since $(\overline{\mathsf{ct}_{\mathcal{S}}}, \mathsf{H}(\overline{\mathsf{ct}_{\mathcal{S}}}))$ is a successful collision. □

Lemma 6 $|S_1 - S_2| \leq \mathsf{Adv}^{\mathsf{kmdh}}_{\mathsf{B},\mathbb{G}_2}(\kappa)$. (*From Difference Lemma* [36])

Proof Game_2 is the same as Game_1 unless A sends a decryption query which is rejected by the condition (2) but passes through the condition (2′). If such a query is issued, we can construct a PPT adversary B solving the KMDH problem. At the beginning, B receives an instance $([\mathbf{B}]_2)$ of the KMDH problem. Then, B randomly selects $\mathbf{A} \xleftarrow{\mathsf{U}} \mathcal{D}_k$ and $\mathbf{X}, \mathbf{Y} \xleftarrow{\mathsf{U}} \mathbb{Z}_p^{(k+1)\times(k+1)}$. For all $\mathsf{id} \in [N]$, B samples $\mathbf{k}_{\mathsf{id}} \xleftarrow{\mathsf{U}} \mathbb{Z}_p^{(k+1)}$. B selects a key-binding secure symmetric encryption scheme $\Pi^{\mathsf{SKE}} = (\mathsf{E}, \mathsf{D})$ with the key space $\mathcal{K} := \mathbb{G}_1$ and a collision-resilient hash function $\mathsf{H} : \{0,1\}^* \to \mathbb{Z}_p$. B sends the following master public key:

$$\mathsf{pk} := \left(\mathcal{PG}, (\mathsf{E}, \mathsf{D}), \mathsf{H}; \begin{matrix} \left[\mathbf{A}^\top\right]_1, \left\{\left[\mathbf{A}^\top\mathbf{k}_{\mathsf{id}}\right]_1\right\}_{\mathsf{id}=1}^N, [\mathbf{B}]_2, \\ \left[\mathbf{A}^\top\mathbf{Y}\right]_1, \left[\mathbf{A}^\top\mathbf{X}\right]_1, [\mathbf{XB}]_2, [\mathbf{YB}]_2 \end{matrix}\right).$$

Note that B knows the master secret key $\mathsf{mk} := \{\mathbf{k}_{\mathsf{id}}\}_{\mathsf{id}=1}^N$.
Key-generation Oracle and Corruption Oracle. B can simulate the oracles since it knows the master secret key.
Challenge. B simulates the challenge as the same as Game_0.
Decryption Oracle. B can simulate the oracle for the same reason as Key-generation and Corruption Oracle. Upon a decryption query $(\mathsf{id}, \mathsf{ct}_{\mathcal{S}} = (\left[\mathbf{u}^\top\right], \mathsf{c}_0, \mathsf{c}_1, \ldots, \mathsf{c}_N, [\boldsymbol{\pi}]_1))$, B

check whether the conditions (2), (2′) hold. If the condition (2) does not hold but (2′) does, B outputs

$$\left[\mathbf{t}^\top := \boldsymbol{\pi} - \mathbf{u}^\top(\mathbf{X} + \alpha \cdot \mathbf{Y})\right]_1.$$

Here, $\left[\mathbf{t}^\top\right]_1$ is a solution to the $\mathcal{D}_k$-KMDH problem since $\mathbf{t}^\top \neq \mathbf{0}$ from (2′) and $\mathbf{t}^\top \in \mathbf{Ker}(\mathbf{B})$ from (2). □

Lemma 7 $\left|S_{2,j-1} - S_{2,j}\right| \leq \frac{1}{p}$. (*From Difference Lemma* [36])

Proof $\mathsf{Game}_{2,j-1}$ is the same as $\mathsf{Game}_{2,j}$ unless A sends the j-th decryption query which is rejected by the condition (2′) but passes through the condition (2″). That is, if the event that the j-th decryption query satisfies $\mathbf{u} \notin \mathrm{span}(\mathbf{A})$ and survives (1), (2′), (3) does not occur, there is no difference between the two games. First, we suppose that $\alpha \neq \alpha^*$ holds for such a query. Then, the decryption query $(\mathsf{id}, \mathsf{ct}_{\mathcal{S}} = (\left[\mathbf{u}^\top\right], \mathsf{c}_0, \mathsf{c}_1, \ldots, \mathsf{c}_N, [\boldsymbol{\pi}]_1))$ must satisfy $\alpha \neq \alpha^*$, $\mathbf{u} \notin \mathrm{span}(\mathbf{A})$ and $[\boldsymbol{\pi}]_1 = \left[\mathbf{u}^\top(\mathbf{X} + \alpha \cdot \mathbf{Y})\mathbf{B}\right]_1$, but this happens with probability at most $\frac{1}{p}$ from the core lemma (Lemma 1 [21]). Note that A never obtain more information than $\mathbf{A}^\top\mathbf{X}, \mathbf{A}^\top\mathbf{Y}$ by the first j-th decryption queries thanks to the condition $\mathbf{u}^* \notin \mathrm{span}(\mathbf{A})$.

Next, we show that the above query must satisfy $\alpha \neq \alpha^*$. Here, if a decryption query survives the condition (3), $\overline{\mathsf{ct}_{\mathcal{S}}} = \mathsf{ct}_{\mathcal{S}_1^*}$ or $\alpha \neq \alpha^*$ holds. Therefore, we need to show that $\overline{\mathsf{ct}_{\mathcal{S}}} \neq \mathsf{ct}_{\mathcal{S}_1^*}$ holds regarding decryption query which survives under the condition (1), (2″), (3) with $\mathbf{u} \notin \mathrm{span}(\mathbf{A})$. We suppose $\overline{\mathsf{ct}_{\mathcal{S}}} = \mathsf{ct}_{\mathcal{S}_1^*}$. We can see that if $\boldsymbol{\pi} = \boldsymbol{\pi}^*$, then the query is rejected by the condition (1), and if $\boldsymbol{\pi} \neq \boldsymbol{\pi}^*$, then the query is rejected by the condition (2′). Thus, since a decryption query with $\overline{\mathsf{ct}_{\mathcal{S}}} = \mathsf{ct}_{\mathcal{S}_1^*}$ cannot survive the conditions, $\alpha \neq \alpha^*$ holds. □

Lemma 8 $\left|S_{2,q_D} - \frac{1}{2}\right| \leq 2 \cdot \mathsf{Adv}^{\mathsf{se}}_{\mathsf{B}}(\kappa)$.

We prove Lemma 8 by considering two cases.

Case (a) : $\mathcal{CD} \cap (\mathcal{S}_0 \cap \mathcal{S}_1) = \emptyset$. In this case, we define the following additional games.

Game_3: This is the same as Game_{2,q_D} except that the challenger samples $\mathsf{c}_{\mathsf{id}} \xleftarrow{\mathsf{U}} \mathbb{G}_1$ for all $\mathsf{id} \in \mathcal{S}_b$ in the challenge ciphertext.

Game_4: This is the same as Game_3 except that the challenger computes $\mathsf{c}_0 = \mathsf{E}_{\mathsf{K}}(0^\kappa)$ in the challenge ciphertext.

Lemma 9 $S_{2,q_D} = S_3$.

Proof We claim that Game_{2,q_D} is statistically indistinguishable from Game_3. In Game_{2,q_D}, A learns information on $\mathbf{k}_{\mathsf{id}}$ ($\mathsf{id} \in \mathcal{S}_b$) only from pk since Decryption Oracle returns for A's queries such that $\mathbf{u} \notin \mathrm{span}(\mathbf{A})$, and $\mathbf{u}^* \notin \mathrm{span}(\mathbf{A})$ holds with overwhelming probability. Then, $\left[\mathbf{u}^{*\top}\mathbf{k}_{\mathsf{id}}\right]_1$ ($\mathsf{id} \in \mathcal{S}_b$) is uniformly distributed over $\mathbb{G}_1$ from the fact that for any $\mathbf{u}^*$ outside the span of $\mathbf{A}$, $\mathbf{u}^{*\top}\mathbf{k}_{\mathsf{id}}$ is uniformly random given $\mathbf{A}^\top\mathbf{k}_{\mathsf{id}}$ where $\mathbf{k}_{\mathsf{id}} \xleftarrow{\mathsf{U}} \mathbb{Z}_p^{(k+1)}$. □

Lemma 10 $|S_3 - S_4| \leq 2 \cdot \mathsf{Adv}^{\mathsf{se}}_{\mathsf{B}}(\kappa)$.

Proof Game_4 is indistinguishable from Game_3 due to the semantic security of (E, D). Finally, we have $S_4 = \frac{1}{2}$ since the challenge ciphertext has no information about b. □

Case (b) : $\mathcal{CD} \cap (\mathcal{S}_0 \cap \mathcal{S}_1) \neq \emptyset$. We define the following game.

Game'_3: This is the same as Game_{2,q_D} except that the challenger samples $\mathsf{c}_{\mathsf{id}} \xleftarrow{\mathsf{U}} \mathbb{G}_1$ for all $\mathsf{id} \in \mathcal{S}_b \backslash \mathcal{S}_{1-b}$.

Lemma 11 $S_{2,q_D} = S_{3'}$.

Proof We claim that Game_{2,q_D} is statistically indistinguishable from Game_3. This follows from the same discussion as in Case (a), that is, the fact that all $\left[\mathbf{u}^{*\top}\mathbf{k}_{\mathsf{id}}\right]_1$ ($\mathsf{id} \in \mathcal{S}_b \backslash \mathcal{S}_{1-b}$) in $\overline{\mathsf{ct}^*_{\mathcal{S}}}$ is uniformly distributed over $\mathbb{G}_1$ conditioned on pk, Key-Generation Oracle and Decryption Oracle. Although c_{id} ($\mathsf{id} \in \mathcal{S}_b \cap \mathcal{S}_{1-b}$) are not changed, no information about b is leaked from the challenge ciphertext since $\mathsf{m}_0 = \mathsf{m}_1$ must hold in this case. We then have $S_{3'} = \frac{1}{2}$. □

Proof of Lemma 8 Let S_a and S_b be the probabilities that A outputs $(\mathcal{S}_0, \mathcal{S}_1)$ in Case (a) and Case (b), respectively. Then, we have

$$\begin{aligned} S_{2,q_D} &= S_3 \cdot S_a + S_{3'} \cdot S_b \\ &\leq |S_3 - S_4| \cdot S_a + S_4 \cdot S_a + S_{3'} \cdot S_b \\ &\leq 2 \cdot \mathsf{Adv}^{\mathsf{se}}_{\mathsf{B}}(\kappa) + \frac{1}{2} \end{aligned}$$

where $S_a + S_b = 1$. □

Proof of Theorem 3 From Lemmas 4–8 we have

$$\begin{aligned} \mathsf{Adv}^{\mathsf{Full\text{-}ANO\text{-}IND\text{-}CCA}}_{\Pi^{\mathsf{BE}},\mathsf{A}}(\kappa, N) \leq\ & \mathsf{Adv}^{\mathsf{mddh}}_{\mathsf{B},\mathbb{G}_1}(\kappa) + \mathsf{Adv}^{\mathsf{hash}}_{\mathsf{B}}(\kappa) + \mathsf{Adv}^{\mathsf{kmdh}}_{\mathsf{B},\mathbb{G}_2}(\kappa) \\ & + q_D \cdot \frac{1}{p} + 2 \cdot \mathsf{Adv}^{\mathsf{se}}_{\mathsf{B}}(\kappa). \end{aligned}$$

□

Here, the above construction has a ciphertext whose size is $(N + 6) \cdot \kappa$ where $k = 1$.[10] Therefore, from Li and Gong's ANO-BE [24] and our Full-ANO-BE scheme, we obtain upper bounds on the ciphertext-size in (Full)-ANO-BE.

From these upper bounds and the asymptotic lower bounds in Sect. 4, we show tight lower bounds on the ciphertext-size in (Full)-ANO-BE.

Theorem 4 *If BE Π^{BE} with properties shown in Sects. 3.2 and 4.1 is Full-ANOat-CCA secure, a non-asymptotic lower bound on the ciphertext-size with any recipient set $\mathcal{S} \subseteq \mathcal{ID}$ is $N \cdot \kappa + o(N \cdot \kappa)$, and our Full-ANO-BE scheme attains the lower bound tightly, which is optimal.*

Theorem 5 *If BE Π^{BE} with properties shown in Sects. 3.2 and 4.1 is ANOat-CCA secure, a non-asymptotic lower bound on the ciphertext-size with any recipient set $\mathcal{S} \subseteq \mathcal{ID}$ is $|\mathcal{S}| \cdot \kappa + o(|\mathcal{S}| \cdot \kappa)$, and the ANO-BE scheme in [24] attains the lower bound tightly, which is optimal.*

6 Atomic broadcast authentication

In this section, we give a syntax of Atomic Broadcast Authentication (AtBA) to formally describe properties satisfied by the existing ABA scheme and derive lower bounds. We further provide security definitions for ABA covered by AtBA.

[10] In this paper, we assume that SKE with key-binding [12] property has a ciphertext of roughly 2 group elements like Li and Gong [24]. See Sect. 6 in [25] for details.

6.1 Syntax of AtBA

Our AtBA describes authentication and verification for each recipient in a designated set performed inside the Auth and Vrfy algorithms of ABA. We define a model for Atomic BA $\Pi^{\mathsf{At\text{-}BA}} = (\mathsf{Setup\text{-}at}, \mathsf{Join\text{-}at}, \mathsf{Auth}, \mathsf{Auth\text{-}at}, \mathsf{Vrfy}, \mathsf{Vrfy\text{-}at})$ as follows, where the Auth and Vrfy are the same as ones of ABA.

1. $\{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta} \leftarrow \mathsf{Setup\text{-}at}(1^\kappa, N)$: a probabilistic algorithm for setup. It takes a security parameter 1^κ and the maximum number of receivers $N \in \mathbb{N}$ as input, and outputs authentication key ak consisting of $|\Delta|$ atomic authentication keys $\{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta}$.
2. $\{\mathsf{vk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma_{\mathsf{id}}} \leftarrow \mathsf{Join\text{-}at}(\{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta}, \mathsf{id})$: a verification key generation algorithm. It takes $\{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta}$ and an identifier $\mathsf{id} \in \mathcal{ID}$, as input, and outputs verification key $\mathsf{vk}_{\mathsf{id}}$ for id consisting of $|\Gamma_{\mathsf{id}}|$ atomic verification keys $\{\mathsf{vk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma_{\mathsf{id}}}$.
3. $\mathsf{cmd}_{\mathcal{S},\mathsf{id}} \leftarrow \mathsf{Auth\text{-}at}(\{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta'}, \mathcal{S}, \mathsf{m}, \mathsf{id}; \mathsf{r})$: an atomic authenticate algorithm. It takes $\{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta'}$, a message $\mathsf{m} \in \mathcal{M}$, a privileged set $\mathcal{S} \subseteq \mathcal{ID}$, an identifier $\mathsf{id} \in \mathcal{ID}$ and randomness $\mathsf{r} \in \mathcal{R}$ as input, and outputs an atomic authenticator $\mathsf{cmd}_{\mathcal{S},\mathsf{id}}$, where $\Delta' \subseteq \Delta$.
4. $\mathsf{m}/\perp \leftarrow \mathsf{Vrfy\text{-}at}(\{\mathsf{vk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma'_{\mathsf{id}}}, \mathsf{cmd}_{\mathcal{S},\mathsf{id}})$: an atomic verification algorithm. It takes a subset of atomic verification keys $\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma'_{\mathsf{id}}}$, and $\mathsf{cmd}_{\mathcal{S},\mathsf{id}}$ as input, and outputs a message m(accept) or $\perp$(reject), where $\Gamma'_{\mathsf{id}} \subseteq \Gamma_{\mathsf{id}}$.

The Setup-at and Join-at are essentially equivalent to the Setup and Join in ABA respectively, except for difference that authentication and verification keys are explicitly divided into multiple sub-elements. As in the case of the Join in BE, we regard the Join-at as being a deterministic algorithm. On the other hand, Auth and Vrfy include Auth-at and Vrfy-at as sub-algorithms, respectively, though they might contain procedures other than the sub-algorithms. Therefore, AtBA includes both (Auth, Vrfy) and (Auth-at, Vrfy-at).

We require a natural property for AtBA that an atomic authenticator $\mathsf{cmd}_{\mathcal{S},\mathsf{id}}$ contained in authenticator $\mathsf{cmd}_{\mathcal{S}}$ will be correctly verified by a verification key $\{\mathsf{vk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma_{\mathsf{id}}}$ of a recipient $\mathsf{id} \in \mathcal{S}$ as follows:

Atomic correctness Fix any $\kappa, N \in \mathbb{N}$, any $\{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta} \leftarrow \mathsf{Setup\text{-}at}(1^\kappa, N)$, any $\mathcal{S} \subseteq \mathcal{ID}$ such that $|\mathcal{S}| \le N$, any $\mathsf{m} \in \mathcal{M}$, any $\{\mathsf{vk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma_{\mathsf{id}}} \leftarrow \mathsf{Join\text{-}at}(\{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta}, \mathsf{id})$, any $\mathsf{r} \xleftarrow{\cup} \mathcal{R}$. Let $\mathsf{cmd}_{\mathcal{S}} \leftarrow \mathsf{Auth}(\{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta}, \mathsf{m}, \mathcal{S}; \mathsf{r})$. Then, there exists some $\Delta' \subseteq \Delta$ for every $\mathsf{id} \in \mathcal{S}$, such that $\mathsf{cmd}_{\mathcal{S},\mathsf{id}} \leftarrow \mathsf{Auth\text{-}at}(\{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta'}, \mathcal{S}, \mathsf{m}, \mathsf{id}; \mathsf{r})$ and $\mathsf{cmd}_{\mathcal{S},\mathsf{id}} \in \mathsf{cmd}_{\mathcal{S}}$. Moreover, the following conditions hold with overwhelming probability:

- $\mathsf{Vrfy}(\{\mathsf{vk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma'_{\mathsf{id}}}, \mathsf{cmd}_{\mathcal{S}}) \to \mathsf{m}$.
- $\mathsf{Vrfy\text{-}at}(\{\mathsf{vk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma'_{\mathsf{id}}}, \mathsf{cmd}_{\mathcal{S},\mathsf{id}}) \to \mathsf{m}$ for some $\Gamma'_{\mathsf{id}} \subseteq \Gamma_{\mathsf{id}}$.

Namely, the above guarantees that (1) a ABA authenticator for $\mathcal{S}$ contains AtBA authenticators for all $\mathsf{id} \in \mathcal{S}$; (2) the ABA authenticator can be correctly verified by the Vrfy, which implies Correctness of ABA; and (3) every AtBA authenticator can be correctly verified by the Vrfy-at. Therefore, Atomic Correctness of AtBA includes Correctness of ABA. Thus, we can say that an ABA scheme is called an AtBA scheme if the Auth and Vrfy includes the Auth-at and Vrfy-at (satisfying the above Atomic Correctness), respectively.

6.2 Security definitions for AtBA

We define anonymity for AtBA in the same way as in BE. In the following, we give definitions of full anonymity (**Full-ANOat-CMA**) and anonymity (**ANOat-CMA**). Security games for

AtBA are the same as those for ABA except that an attacker obtains verification keys and a challenge authenticator is explicitly-devided into multiple sub-elements. Essentially, there is no difference in information the attacker obtains between security games for BA and those for AtBA. Therefore, we consider (Full-)ANOat-CMA defined below to be equivalent security notions as (full) anonymity.

Let A be any PPT adversary against Full-ANOat-CMA security. We consider an experiment $\mathsf{Exp}^{\mathsf{Full\text{-}ANOat\text{-}CMA}}_{\Pi^{\mathsf{At\text{-}BA}},\mathsf{A}}(\kappa, N)$ between a challenger C and A. Let $\mathsf{Exp}^{\mathsf{Full\text{-}ANOat\text{-}CMA}}_{\Pi^{\mathsf{At\text{-}BA}},\mathsf{A}}$ be the experiment with the following changes to Key-generation Query and Corruption Query in experiment $\mathsf{Exp}^{\mathsf{Full\text{-}ANO\text{-}CMA}}_{\Pi^{\mathsf{ABA}},\mathsf{A}}$.

- Key-generation Query: Upon a query $\mathsf{id} \in \mathcal{ID}$ from A, C adds id to $\mathcal{D}$ and generates $\{\mathsf{vk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma_{\mathsf{id}}} \leftarrow \mathsf{Join\text{-}at}(\mathsf{ak}, \mathsf{id})$, not $\mathsf{vk}_{\mathsf{id}} \leftarrow \mathsf{Join}(\mathsf{ak}, \mathsf{id})$.
- Corruption Query: Upon a query $\mathsf{id} \in \mathcal{D}$ from A, C adds id to $\mathcal{CD}$, and returns $\{\mathsf{vk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma_{\mathsf{id}}}$ to A, not $\mathsf{vk}_{\mathsf{id}}$.

We also define ANOat-CMA with an experiment $\mathsf{Exp}^{\mathsf{ANOat\text{-}CMA}}_{\Pi^{\mathsf{At\text{-}BA}},\mathsf{A}}(\kappa, N)$ which is the same as $\mathsf{Exp}^{\mathsf{Full\text{-}ANOat\text{-}CMA}}_{\Pi^{\mathsf{At\text{-}BA}},\mathsf{A}}(\kappa, N)$ except for the following additional condition of the restriction for challenge query: $|\mathcal{S}_0| = |\mathcal{S}_1|$.

Definition 11 ((Full-)ANOat-CMA) We say $\Pi^{\mathsf{At\text{-}BA}}$ is X secure (X $\in$ Full-ANOat-CMA, ANOat-CMA) if for any PPT adversary A, for all sufficiently-large $\kappa \in \mathbb{N}$ and all $N \in \mathbb{N}$, it holds that $\mathsf{Adv}^{X}_{\Pi^{\mathsf{At\text{-}BA}},\mathsf{A}}(\kappa, N) < \mathsf{negl}(\kappa)$, where $\mathsf{Adv}^{X}_{\Pi^{\mathsf{At\text{-}BA}},\mathsf{A}}(\kappa, N) := \left|\Pr\left[\mathsf{Exp}^{X}_{\Pi^{\mathsf{At\text{-}BA}},\mathsf{A}}(\kappa, N) \to 1\right] - \frac{1}{2}\right|$.

6.3 Properties in an existing ABA scheme

In this section, we describe four properties that holds for an existing ABA scheme. The four properties are as follows.

Property 5 Authenticator $\mathsf{cmd}_{\mathcal{S}}$ output from the Auth algorithm consists of atomic authenticators $\mathsf{cmd}_{\mathcal{S},\mathsf{id}}$ obtained by the $\mathsf{Auth\text{-}at}$ algorithm, and other elements. In other words, let a set of atomic authenticators contained in $\mathsf{cmd}_{\mathcal{S}}$ be $\{\mathsf{cmd}_{\mathcal{S},\mathsf{id}}\}_{\mathsf{id}\in\mathcal{S}}$, and let the union of $\{\mathsf{cmd}_{\mathcal{S},\mathsf{id}}\}_{\mathsf{id}\in\mathcal{S}}$ and some elements contained in $\mathsf{cmd}_{\mathcal{S}}$ be $\{\mathsf{cmd}^{(\theta)}_{\mathcal{S}}\}_{\theta\in[\beta_{\mathcal{S}}]}$, it holds that $\{\mathsf{cmd}_{\mathcal{S},\mathsf{id}}\}_{\mathsf{id}\in\mathcal{S}} \subseteq \{\mathsf{cmd}^{(\theta)}_{\mathcal{S}}\}_{\theta\in[\beta_{\mathcal{S}}]} \subseteq \mathsf{cmd}_{\mathcal{S}}$. Here, the randomness r input to the $\mathsf{Auth\text{-}at}$ is the same when generating $\{\mathsf{cmd}_{\mathcal{S},\mathsf{id}}\}_{\mathsf{id}\in\mathcal{S}}$ respectively. Also, inside the Vrfy algorithm, the $\mathsf{Vrfy\text{-}at}$ algorithm takes an atomic authenticator and a set of atomic verification keys as input, and outputs a message. If $\mathsf{cmd}_{\mathcal{S}}$ is a valid authenticator, then there is an atomic authenticator $\mathsf{cmd}^{(\theta)}_{\mathcal{S}}$ in $\mathsf{cmd}_{\mathcal{S}}$ that can be verified using a subset of atomic verification keys of a recipient id in $\mathcal{S}$. Formally, we require the following property for AtBA $\Pi^{\mathsf{At\text{-}BA}}$:

For all $\kappa, N \in \mathbb{N}$, all $\mathsf{ak} \leftarrow \mathsf{Setup}(1^{\kappa}, N)$, all $\mathsf{m} \in \mathcal{M}$, all $\mathcal{S} \subseteq \mathcal{ID}$ such that $|\mathcal{S}| \leq N$, all $\mathsf{id} \in \mathcal{ID}$, all $\{\mathsf{vk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma_{\mathsf{id}}} \leftarrow \mathsf{Join\text{-}at}(\mathsf{ak}, \mathsf{id})$, all $\mathsf{r} \xleftarrow{\mathsf{U}} \mathcal{R}$, all $\{\mathsf{cmd}^{(\theta)}_{\mathcal{S}}\}_{\theta\in[\beta_{\mathcal{S}}]} \subseteq \mathsf{cmd}_{\mathcal{S}} \leftarrow \mathsf{Auth}(\mathsf{ak}, \mathsf{m}, \mathcal{S}; \mathsf{r})$, if $\mathsf{id} \in \mathcal{S}$, then for some $\Gamma'_{\mathsf{id}} \subseteq \Gamma_{\mathsf{id}}$, there exists $\theta \in [\beta_{\mathcal{S}}]$ such that $\mathsf{m} \leftarrow \mathsf{Vrfy\text{-}at}(\{\mathsf{vk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma'_{\mathsf{id}}}, \mathsf{cmd}^{(\theta)}_{\mathcal{S}})$. If $\mathsf{id} \notin \mathcal{S}$, then for all $\Gamma'_{\mathsf{id}} \subseteq \Gamma_{\mathsf{id}}$, there is no $\theta \in [\beta_{\mathcal{S}}]$ such that $\mathsf{m} \leftarrow \mathsf{Vrfy\text{-}at}(\{\mathsf{vk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma'_{\mathsf{id}}}, \mathsf{cmd}^{(\theta)}_{\mathcal{S}})$.

Property 6 When generating $\mathsf{cmd}_{\mathcal{S},\mathsf{id}}$ such that $\mathsf{m} \leftarrow \mathsf{Vrfy\text{-}at}(\{\mathsf{vk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma'_{\mathsf{id}}}, \mathsf{cmd}_{\mathcal{S},\mathsf{id}})$ for some $\gamma \in \Gamma'_{\mathsf{id}}$, let $\Delta^{*}_{\mathsf{id},\mathcal{S},\mathsf{m}}$ be a minimum subset of atomic authentication keys required for

the input to Auth-at. In this case, $\Delta^*_{\mathsf{id},\mathcal{S},\mathsf{m}}$ is uniquely determined by pairs of the recipient's identifier, the message, and the set $(\mathsf{id}, \mathcal{S}, \mathsf{m})$ to input to Auth-at.

Property 7 When $\mathsf{m} \leftarrow \mathsf{Vrfy\text{-}at}(\{\mathsf{vk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma'_{\mathsf{id}}}, \mathsf{cmd}_{\mathcal{S},\mathsf{id}})$ holds, let $\Gamma^*_{\mathsf{id},\mathcal{S}}$ be a minimum subset of atomic verification keys required for the input to Vrfy-at. In this case, $\Gamma^*_{\mathsf{id},\mathcal{S}}$ is uniquely determined by pairs of the recipient's identifier, and the set $(\mathsf{id}, \mathcal{S})$ to input to Auth-at when generating $\mathsf{cmd}_{\mathcal{S},\mathsf{id}}$.

Property 8 For all $(\mathsf{ak}, \{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta}) \leftarrow \mathsf{Setup}(1^\kappa, N)$, $\mathsf{id}, \mathsf{id}' \in \mathcal{ID}$, all $\mathcal{S}$ such that $\{\mathsf{id}, \mathsf{id}'\} \subseteq \mathcal{S}$, all $\mathsf{m} \in \mathcal{M}$, $\mathsf{r} \in \mathcal{R}$, all $\mathsf{cmd}_{\mathcal{S},\mathsf{id}} \leftarrow \mathsf{Auth\text{-}at}(\{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id},\mathcal{S},\mathsf{m}}}, \mathsf{id}, \mathsf{m}, \mathcal{S}; \mathsf{r})$, $\mathsf{cmd}_{\mathcal{S},\mathsf{id}'} \leftarrow \mathsf{Auth\text{-}at}(\{\mathsf{ak}^{(\delta')}\}_{\delta'\in\Delta^*_{\mathsf{id}',\mathcal{S},\mathsf{m}}}, \mathsf{id}', \mathsf{m}, \mathcal{S}; \mathsf{r})$, if $\mathsf{cmd}_{\mathcal{S},\mathsf{id}} = \mathsf{cmd}_{\mathcal{S},\mathsf{id}'}$ holds, then we have $\{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id},\mathcal{S},\mathsf{m}}} = \{\mathsf{ak}^{(\delta')}\}_{\delta'\in\Delta^*_{\mathsf{id}',\mathcal{S},\mathsf{m}}}$ with overwhelming probability.

Here, we can see that the existing ABA scheme [37] satisfies the above properties in a similar way in Sect. 3.2.

7 Asymptotic lower bounds in anonymous broadcast authentication

In order to derive lower bounds for ANO-BA and Full-ANO-BA, we assume a property that "a minimum subset of atomic verification keys used to verify authenticators is uniquely determined by a subset of authentication keys used to generate the authenticator." Specifically, we consider the following property for ANO-BA and Full-ANO-BA:

Assumption 3 When $\{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta} \leftarrow \mathsf{Setup}(1^\kappa, N)$ is generated, we denote $\mathcal{AK}^*$ as a set of all authentication keys, namely $\mathcal{AK}^* := \{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta}$. And, when $\{\mathsf{vk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma_{\mathsf{id}}} \leftarrow \mathsf{Join\text{-}at}(\mathsf{ak}, \mathsf{id})$ is generated, $\mathcal{VK}^*$ denotes a family of the minimum subsets of atomic verification keys to be input to the Vrfy-at, namely $\mathcal{VK}^* := \{\{\mathsf{vk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma\in\Gamma^*_{\mathsf{id},\mathcal{S}}}\}_{\mathsf{id}\in\mathcal{ID},\mathcal{S}\subseteq\mathcal{ID}}$. Here, we note that $\mathcal{VK}^*$ is uniquely determined, since Join-at is a deterministic algorithm. At this time, for all $\mathsf{id} \in \mathcal{ID}$, all $\mathcal{S} \subseteq \mathcal{ID}$, all $\mathsf{m} \in \mathcal{M}$, all $\mathsf{r} \in \mathcal{R}$, all $\mathsf{ak}' \in 2^{\mathcal{AK}^*}$, all $\mathsf{cmd}_{\mathcal{S},\mathsf{id}} \leftarrow \mathsf{Auth\text{-}at}(\mathsf{ak}', \mathsf{id}, \mathsf{m}, \mathcal{S}; \mathsf{r})$, a set of atomic verification keys $\mathsf{vk}' \in \mathcal{VK}^* \cup \{\perp\}$ such that $\mathsf{m} \leftarrow \mathsf{Vrfy\text{-}at}(\mathsf{vk}', \mathsf{cmd}_{\mathcal{S},\mathsf{id}})$ is uniquely determined by the set of atomic authentication keys ak'.

The above property holds for Watanabe et al.'s ANO-BA and Full-ANO-BA schemes [37], which is a generic construction using message authentication code and pseudo-random function. Since it can be shown that they satisfies the above property in the same way as the ANO-BE scheme of Libert et al. [25], we omit a detailed discussion here.

7.1 Lower bounds in ANOat-CMA secure AtBA

First, we show two lemmas, Lemmas 12 and 13, for ANOat-CMA secure AtBA with Properties 5, 6, 7 and 8 described in Sect. 6.3. In Lemma 12, we show that "if an AtBA is ANOat-CMA secure, then for authenticators with a set $\mathcal{S}_0, \mathcal{S}_1$ whose size is equal, sets of atomic verification keys used by a receipient id for each verification is equal with overwhelming probability." Then, in Lemma 13, we show that "if an AtBA is ANOat-CMA secure, then for any set $\mathcal{S}$ with more than two elements, recipients $\mathsf{id}, \mathsf{id}' \in \mathcal{S}$ must not share a set of atomic verification keys used to verify $\mathsf{cmd}_{\mathcal{S}}$ with overwhelming probability."

Then, for ANOat-CMA secure AtBA with the property described in Assumption 3, we will derive a lower bound on authenticator-size by Theorem 6.

For convenience, for any $\mathcal{S}_0, \mathcal{S}_1 \subseteq \mathcal{ID}$, we call $(\mathcal{S}_0, \mathcal{S}_1)$ *challengeable sets* if it can be used for a challenge query in the ANOat-CMA game $\mathsf{Exp}^{\mathsf{ANOat\text{-}CMA}}_{\Pi^{\mathsf{At\text{-}BA}},\mathsf{A}}$.

Lemma 12 *If AtBA* $\Pi^{\mathsf{At\text{-}BA}}$ *is ANOat-CMA secure, no PPT adversary* A *in the ANOat-CMA game can find* $\mathsf{id} \in \mathcal{ID}$ *and challengable sets* $(\mathcal{S}_0, \mathcal{S}_1) \in \left(2^{\mathcal{D}}_{\leq N}\right)^2$ *such that* $\mathsf{id} \in \mathcal{S}_0 \cap \mathcal{S}_1$, $|\mathcal{S}_0| = |\mathcal{S}_1|$, *and* $\{\mathsf{vk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}_0}} \neq \{\mathsf{vk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}_1}}$ *with non-negligible probability.*

Proof We show this lemma by contraposition. Suppose that there exists a PPT adversary A that can find $(\mathsf{id}, \mathcal{S}_0, \mathcal{S}_1)$ in the ANOat-CMA game such that $(\mathcal{S}_0, \mathcal{S}_1)$ is challengeable sets and it holds that $\mathsf{id} \in \mathcal{S}_0 \cap \mathcal{S}_1$, $|\mathcal{S}_0| = |\mathcal{S}_1|$, and $\{\mathsf{vk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}_0}} \neq \{\mathsf{vk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}_1}}$ with non-negligible probability. Note that by Property 3, $\Gamma^*_{\mathsf{id},\mathcal{S}_0}$ and $\Gamma^*_{\mathsf{id},\mathcal{S}_1}$ are uniquely determined. Then, A can break ANOat-CMA security as follows. During the ANOat-CMA game, A can find $(\mathsf{id}^*, \mathcal{S}_0, \mathcal{S}_1)$ such that $\{\mathsf{vk}^{(\gamma)}_{\mathsf{id}^*}\}_{\gamma \in \Gamma^*_{\mathsf{id}^*,\mathcal{S}_0}} \neq \{\mathsf{vk}^{(\gamma)}_{\mathsf{id}^*}\}_{\gamma \in \Gamma^*_{\mathsf{id}^*,\mathcal{S}_1}}$. A then issues key-generation queries for every $\mathsf{id} \in \mathcal{S}_0 \cup \mathcal{S}_1$ and a corruption query for id^* (if A has not done them yet), and obtains a verification key $\{\mathsf{vk}^{(\gamma)}_{\mathsf{id}^*}\}_{\gamma \in \Gamma_{\mathsf{id}^*}}$. A then issues a challenge query $(\mathsf{m}, \mathcal{S}_0, \mathcal{S}_1)$ to obtain $\{\mathsf{cmd}^{(\theta)}_{\mathcal{S}_b}\}_{\theta \in [\beta_{\mathcal{S}_b}]} \subseteq \mathsf{cmd}_{\mathcal{S}_b}$. Note that A can get the verification key for id^* since $\mathsf{id}^* \in \mathcal{S}_0 \cap \mathcal{S}_1$ and $(\mathcal{S}_0, \mathcal{S}_1)$ can be used for the challenge query. Finally, A outputs $b' = 0$ if there exists $\theta \in [\beta_{\mathcal{S}_b}]$ such that $\mathsf{m} \leftarrow \mathsf{Vrfy\text{-}at}(\{\mathsf{vk}^{(\gamma)}_{\mathsf{id}^*}\}_{\gamma \in \Gamma^*_{\mathsf{id}^*,\mathcal{S}_0}}, \mathsf{cmd}^{(\theta)}_{\mathcal{S}_b})$, and $b' = 1$ otherwise. In this case, A can output b' such that $b = b'$ with non-negligible probability. □

Lemma 13 *If AtBA* $\Pi^{\mathsf{At\text{-}BA}}$ *is ANOat-CMA secure, no PPT adversary* A *in the ANOat-CMA game can find* $(\mathsf{id}, \mathsf{id}', \mathcal{S}) \in \mathcal{ID}^2 \times 2^{\mathcal{D}}_{\leq N}$ *such that* $\mathsf{id}, \mathsf{id}' \in \mathcal{S}$ *and* $\{\mathsf{vk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}}} \neq \{\mathsf{vk}^{(\gamma')}_{\mathsf{id}'}\}_{\gamma' \in \Gamma^*_{\mathsf{id}',\mathcal{S}}}$ *with non-negligible probability.*

Proof Assume on the contrary that there exists a PPT adversary A that can find $(\mathsf{id}, \mathsf{id}', \mathcal{S})$ such that $\mathsf{id}, \mathsf{id}' \in \mathcal{S}$ and $\{\mathsf{vk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}}} = \{\mathsf{vk}^{(\gamma')}_{\mathsf{id}'}\}_{\gamma' \in \Gamma^*_{\mathsf{id}',\mathcal{S}}}$ with non-negligible probability. Note that by Property 7, $\Gamma^*_{\mathsf{id},\mathcal{S}}$ and $\Gamma^*_{\mathsf{id}',\mathcal{S}}$ are uniquely determined. Then, we will show that it contradicts Property 5 of AtBA in Sect. 6.3) for any $\mathcal{S}'$ such that $\mathsf{id} \in \mathcal{S}'$, $\mathsf{id}' \notin \mathcal{S}'$, and $|\mathcal{S}| = |\mathcal{S}'|$. Suppose that A has atomic verification keys $\{\mathsf{vk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma_{\mathsf{id}}}$ and $\{\mathsf{vk}^{(\gamma')}_{\mathsf{id}'}\}_{\gamma' \in \Gamma_{\mathsf{id}'}}$ by key-generation queries and corruption queries. Since $\mathsf{id} \in \mathcal{S}'$, we have $\mathsf{m} \leftarrow \mathsf{Vrfy\text{-}at}(\{\mathsf{vk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}'}}, \mathsf{cmd}_{\mathcal{S}',\mathsf{id}})$. From Lemma 12, we have $\{\mathsf{vk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}'}} = \{\mathsf{vk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}}}$ with overwhelming probability as discussed in Lemma 3. Hence, we have $\mathsf{m} \leftarrow \mathsf{Vrfy\text{-}at}(\{\mathsf{vk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}}}, \mathsf{cmd}_{\mathcal{S}',\mathsf{id}})$. Here, since $\{\mathsf{vk}^{(\gamma)}_{\mathsf{id}}\}_{\gamma \in \Gamma^*_{\mathsf{id},\mathcal{S}}} = \{\mathsf{vk}^{(\gamma')}_{\mathsf{id}'}\}_{\gamma' \in \Gamma^*_{\mathsf{id}',\mathcal{S}}}$ from the assumption, we have $\mathsf{m} \leftarrow \mathsf{Vrfy\text{-}at}(\{\mathsf{vk}^{(\gamma')}_{\mathsf{id}'}\}_{\gamma' \in \Gamma^*_{\mathsf{id}',\mathcal{S}}}, \mathsf{cmd}_{\mathcal{S}',\mathsf{id}})$. However, since $\mathsf{id}' \notin \mathcal{S}'$ holds, the above contradicts Property 5. □

In the following, we derive a lower bound on authenticator-size in ANOat-CMA secure AtBA with the property described in Assumption 3. Specifically, we show the statement: When there exists a set $\mathcal{S}$ such that the number of atomic authenticators $\mathsf{cmd}_{\mathcal{S}}$ contained in $\mathsf{cmd}_{\mathcal{S}}$ is less than $|\mathcal{S}|$ with non-negligible probability, a contradiction occurs for Lemma 13.

Theorem 6 *If AtBA* $\Pi^{\mathsf{At\text{-}BA}}$ *with the property shown in Assumption 3 is ANOat-CMA secure, the size of authenticators for any recipient set* $\mathcal{S} \in 2^{\mathcal{ID}}_{\leq N}$ *and any message* $\mathsf{m} \in \mathcal{M}$ *is* $\Omega(|\mathcal{S}| \cdot k)$

with overwhelming probability, where $k = \min_{\mathcal{S}\subseteq\mathcal{ID},\theta\in[\beta_{\mathcal{S}}]} |\mathsf{cmd}_{\mathcal{S}}^{(\theta)}|$ *and the probability is taken over the internal randomness of the* Setup-at, Auth, *and* Auth-at. *In other words, if AtBA* $\Pi^{\mathsf{At\text{-}BA}}$ *is ANOat-CMA secure and has the property in Assumption 3, for any recipient set* $\mathcal{S} \in 2^{\mathcal{ID}}_{\leq N}$ *and any message* $\mathsf{m} \in \mathcal{M}$, *the* Auth *outputs a authenticator of size* $\Omega(|\mathcal{S}| \cdot k)$ *with overwhelming probability.*

Proof For some set of recipients $\mathcal{S}^* \in 2^{\mathcal{ID}}_{\leq N}$ and message $\mathsf{m}^* \in \mathcal{M}$, we assume that with non-negligible probability, the Auth outputs $\mathsf{cmd}_{\mathcal{S}^*} = \{\mathsf{cmd}_{\mathcal{S}^*}^{(\theta)}\}_{\theta\in[\beta_{\mathcal{S}^*}]} \leftarrow \mathsf{Auth}(\{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta}, \mathsf{m}^*, \mathcal{S}^*; \mathsf{r}^*)$ and $\beta_{\mathcal{S}^*} < |\mathcal{S}^*|$. Let A be any fixed PPT adversary against the ANOat-CMA game. Then, as discussed in Theorem 1, A can identify such $(\mathcal{S}^*, \mathsf{m}^*)$ with non-negligible probability since A knows the concrete procedure of Auth (since it should be public due to Kerckhoffs' principle). We then show that A can find $(\mathsf{id}, \mathsf{id}', \mathcal{S}^*)$ that contradicts Lemma 13. Now, from $\beta_{\mathcal{S}^*} \geq 1$, we consider that $|\mathcal{S}^*| \geq 2$ holds. From $\beta_{\mathcal{S}^*} < |\mathcal{S}^*|$, for a set of atomic authenticators $\{\mathsf{cmd}_{\mathcal{S}^*}^{(\theta)}\}_{\theta\in\beta_{\mathcal{S}^*}}$, there exists at least one atomic authenticator $\mathsf{cmd}_{\mathcal{S}^*}^{(\theta^*)}$ that can be decrypted by two recipients $\mathsf{id}, \mathsf{id}' \in \mathcal{S}^*$. That is, for $\mathsf{id}, \mathsf{id}' \in \mathcal{S}^*$, it holds that $\mathsf{cmd}_{\mathcal{S}^*}^{(\theta^*)} = \mathsf{cmd}_{\mathcal{S},\mathsf{id}} = \mathsf{cmd}_{\mathcal{S},\mathsf{id}'}$, where $\mathsf{cmd}_{\mathcal{S},\mathsf{id}}, \mathsf{cmd}_{\mathcal{S},\mathsf{id}'}$ is generated by

$$\mathsf{cmd}_{\mathcal{S},\mathsf{id}} \leftarrow \mathsf{Auth\text{-}at}(\{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id},\mathcal{S}^*,\mathsf{m}^*}}, \mathsf{id}, \mathsf{m}^*, \mathcal{S}^*; \mathsf{r}^*),$$
$$\mathsf{cmd}_{\mathcal{S},\mathsf{id}'} \leftarrow \mathsf{Auth\text{-}at}(\{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id}',\mathcal{S}^*,\mathsf{m}^*}}, \mathsf{id}', \mathsf{m}^*, \mathcal{S}^*; \mathsf{r}^*),$$

where r^* is the same randomness in Auth above. Note that by Property 6, $\Delta^*_{\mathsf{id},\mathcal{S}^*,\mathsf{m}^*}$ and $\Delta^*_{\mathsf{id}',\mathcal{S}^*,\mathsf{m}^*}$ are uniquely determined, and by Property 8, it holds $\{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id},\mathcal{S}^*,\mathsf{m}^*}} = \{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id}',\mathcal{S}^*,\mathsf{m}^*}}$. In addition, by Atomic Correctness and Property 5, we have

$$\mathsf{m}^* \leftarrow \mathsf{Vrfy\text{-}at}(\{\mathsf{vk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma^*_{\mathsf{id},\mathcal{S}^*}}, \mathsf{cmd}_{\mathcal{S}^*}^{(\theta^*)}),$$
$$\mathsf{m}^* \leftarrow \mathsf{Vrfy\text{-}at}(\{\mathsf{vk}_{\mathsf{id}'}^{(\gamma')}\}_{\gamma'\in\Gamma^*_{\mathsf{id}',\mathcal{S}^*}}, \mathsf{cmd}_{\mathcal{S}^*}^{(\theta^*)}).$$

Note that by Property 7, $\{\mathsf{vk}_{\mathsf{id}'}^{(\gamma')}\}_{\gamma'\in\Gamma^*_{\mathsf{id},\mathcal{S}^*}}$ and $\{\mathsf{vk}_{\mathsf{id}'}^{(\gamma')}\}_{\gamma'\in\Gamma^*_{\mathsf{id}',\mathcal{S}^*}}$ are uniquely determined. From Assumption 3, $\{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id},\mathcal{S}^*,\mathsf{m}^*}}$ and $\{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id}',\mathcal{S}^*,\mathsf{m}^*}}$ uniquely determine $\{\mathsf{vk}_{\mathsf{id}}^{(\gamma')}\}_{\gamma'\in\Gamma^*_{\mathsf{id},\mathcal{S}^*}}$ and $\{\mathsf{vk}_{\mathsf{id}'}^{(\gamma')}\}_{\gamma'\in\Gamma^*_{\mathsf{id}',\mathcal{S}^*}}$ such that

$$\mathsf{m}^* \leftarrow \mathsf{Vrfy\text{-}at}(\{\mathsf{vk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma^*_{\mathsf{id},\mathcal{S}^*}}, \mathsf{Auth\text{-}at}(\{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id},\mathcal{S}^*,\mathsf{m}^*}}, \mathsf{id}, \mathsf{m}^*, \mathcal{S}^*; \mathsf{r}^*)),$$
$$\mathsf{m}^* \leftarrow \mathsf{Vrfy\text{-}at}(\{\mathsf{vk}_{\mathsf{id}'}^{(\gamma)}\}_{\gamma\in\Gamma^*_{\mathsf{id}',\mathcal{S}^*}}, \mathsf{Auth\text{-}at}(\{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id}',\mathcal{S}^*,\mathsf{m}^*}}, \mathsf{id}', \mathsf{m}^*, \mathcal{S}^*; \mathsf{r}^*)),$$

respectively. As mentioned above, it holds $\{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id},\mathcal{S}^*,\mathsf{m}^*}} = \{\mathsf{ak}^{(\delta)}\}_{\delta\in\Delta^*_{\mathsf{id}',\mathcal{S}^*,\mathsf{m}^*}}$. Therefore, despite ANOat-CMA security of $\Pi^{\mathsf{At\text{-}BA}}$, A can obtain $\{\mathsf{vk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma\in\Gamma^*_{\mathsf{id},\mathcal{S}^*}} = \{\mathsf{vk}_{\mathsf{id}'}^{(\gamma')}\}_{\gamma'\in\Gamma^*_{\mathsf{id}',\mathcal{S}^*}}$, which contradicts Lemma 13. □

7.2 Lower bounds in Full-ANOat-CMA secure AtBA

We derive a lower bound on authenticator size in Theorem 7 for Full-ANOat-CMA secure AtBA with the property described in Assumption 3, using Theorem 6.

Theorem 7 *If AtBA* $\Pi^{\mathsf{At\text{-}BA}}$ *with the property shown in Assumption 3 is Full-ANOat-CMA secure, the size of authenticators for any recipient set* $\mathcal{S} \in 2^{\mathcal{ID}}_{\leq N}$ *and any message* $\mathsf{m} \in \mathcal{M}$ *is* $\Omega(N \cdot k)$ *with overwhelming probability, where* $k = \min_{\mathcal{S} \subseteq \mathcal{ID}, \theta \in [\beta_{\mathcal{S}}]} |\mathsf{cmd}^{(\theta)}_{\mathcal{S}}|$ *and the probability is taken over the internal randomness of the* Setup-at, Auth, *and* Auth-at. *In other words, if AtBA* $\Pi^{\mathsf{At\text{-}BA}}$ *is Full-ANOat-CMA secure and has the property in Assumption 3, for any recipient set* $\mathcal{S} \in 2^{\mathcal{ID}}_{\leq N}$ *and any message* $\mathsf{m} \in \mathcal{M}$, *the* Auth *outputs a authenticator of size* $\Omega(N \cdot k)$ *with overwhelming probability.*

Proof Since Full-ANOat-CMA security implies ANOat-CMA security, for any $\mathcal{S} \in 2^{\mathcal{ID}}_{\leq N}$, we at least have $\Omega(|\mathcal{S}| \cdot \kappa)$ with overwhelming probability from Theorem 6. Now, we assume that for some set of recipients $\mathcal{S}^* \in 2^{\mathcal{ID}}_{\leq N}$ and message $\mathsf{m}^* \in \mathcal{M}$, Auth outputs $\mathsf{cmd}_{\mathcal{S}^*} = \{\mathsf{cmd}^{(\theta)}_{\mathcal{S}^*}\}_{\theta \in [\beta_{\mathcal{S}^*}]} \leftarrow \mathsf{Auth}(\{\mathsf{pk}^{(\delta)}\}_{\delta \in \Delta}, \mathsf{m}^*, \mathcal{S}^*; \mathsf{r}^*)$ such that $|\mathcal{S}^*| \leq \beta_{\mathcal{S}^*} < N$, with non-negligible probability. Let A be any fixed PPT adversary against the Full-ANOat-CMA game. Then, A can identify such $(\mathcal{S}^*, \mathsf{m}^*)$ with non-negligible probability since A knows the concrete procedure of Auth (since it should be public due to Kerckhoffs' principle). A then issues a challenge query $(\mathsf{m}^*, \mathcal{S}^*, \mathcal{S})$, where $\mathcal{S} = [N]$ and $\mathcal{S}^*$ is any set in $2^{\mathcal{ID}}_{\leq N} \setminus [N]$. Here, from the assumption that $|\mathcal{S}^*| \leq \beta_{\mathcal{S}^*} < N$, A can trivially break Full-ANOat-CMA, but it contradicts the premise. Thus, the size of authenticators for any $\mathcal{S} \in 2^{\mathcal{ID}}_{\leq N}$ must be equal to that of authenticators for $[N]$ at least, i.e., $\Omega(N \cdot \kappa)$. □

8 Non-asymptotic bounds and optimal constructions of ABA

We show (non-asymptotic) upper and lower bounds on the authenticator-size in ABA. Specifically, we propose *optimal* constructions of ABA with anonymity and full-anonymity, respectively, to show non-asymptotic upper bounds of the authenticator size.

Our UF-CMA secure and Full-ANO-CMA secure ABA is as follows.

- $\mathsf{Setup}(1^\kappa, N)$: For all $\mathsf{id} \in [N]$, run $\mathsf{K_{id}} \leftarrow \mathsf{MAC.Gen}(1^\kappa)$ to get $\{\mathsf{K_{id}}\}_{\mathsf{id} \in [N]}$. Output the authentication key $\mathsf{ak} := \{\mathsf{K_{id}}\}_{\mathsf{id} \in [N]}$.
- $\mathsf{Join}(\mathsf{mk}, \mathsf{id})$: Output the verification key $\mathsf{vk_{id}} := \mathsf{K_{id}}$.
- $\mathsf{Auth}(\mathsf{ak}, \mathsf{m}, \mathcal{S})$: Let n be the number of recipients currently participating in the system, and suppose that $\mathsf{vk}_{\mathsf{id}_1}, \ldots, \mathsf{vk}_{\mathsf{id}_n}$ have been generated by Join so far. Let $\mathsf{ak} = \{\mathsf{K_{id}}\}_{\mathsf{id} \in [N]}$, $x \xleftarrow{\cup} \mathcal{R}$, and compute the following for all $\mathsf{id} \in [N]$:

$$\begin{cases} \tau \leftarrow \mathsf{MAC.Auth}(\mathsf{K_{id}}, \mathsf{m}||x), & \text{if } \mathsf{id} \in \mathcal{S}, \\ \tau \leftarrow \mathsf{MAC.Auth}(\mathsf{K_{id}}, 0^\kappa||x), & \text{if } \mathsf{id} \notin \mathcal{S}. \end{cases}$$

  Here, $\mathcal{R}$ is a random space. Choose a random permutation σ from $\{\sigma_i : [N] \to [N]\}_{i \in \{0,1\}^\kappa}$ and the authenticator is

$$\mathsf{cmd}_{\mathcal{S}} := (\mathsf{m}, x, \tau_{\sigma(1)}, \ldots, \tau_{\sigma(N)}).$$

- $\mathsf{Vrfy}(\mathsf{vk_{id}}, \mathsf{cmd}_{\mathcal{S}})$: Let $\mathsf{vk_{id}} = \mathsf{K_{id}}, \mathsf{cmd}_{\mathcal{S}} = (\mathsf{m}, x, \tau_1, \ldots, \tau_N)$. Do the following two steps from $j := 1$.
  - Run $\mathsf{MAC.Vrfy}(\mathsf{K_{id}}, \tau_j, \mathsf{m}||x)$ and if its output is $\top$, return m and halt; otherwise, go to the second step.
  - If $j = N$, return $\perp$ and halt; otherwise, do the first step with $j := j + 1$.

A proof of UF-CMA security in the above construction is intuitively almost identical to an evaluation of a probability that an adversary forges a MAC in a multi-key setting. However, due to an existence of the Key Derivation Oracle, we cannot simply apply the standard hybrid argument for the number of recipients assuming pseudo-randomness for Π^{MAC} (when the hybrid argument can be applied, i.e., there is no Key Derivation Oracle, we can prove UF-CMA security assuming pseudo-randomness for Π^{MAC} in a single-key setting.). Although it is not impossible to prove the security with the Key Derivation Oracle in the standard model assuming pseudo-randomness for Π^{MAC} in a multi-key setting, it is known to be a very inefficient reduction [28]. A simple proof is possible in the non-standard model where MAC.Auth is regarded as a public random function (Random Oracle). Therefore, in this paper, we give a proof under an assumption that MAC.Auth is the public random function.

Theorem 8 *Assume that* MAC.Auth *is a public random function. If* Π^{MAC} *is UF-CMA secure, the above construction is UF-CMA secure and Full-ANO-CMA secure.*

The UF-CMA security can be proved by the H-Coefficient technique [31], which is a standard framework to analyze the security of symmetric key cryptographic modes (See [8] for example. However, [8] does not deal with a multi-key setting and a decision game because they show a proof for a security that combines PRF and UF-CMA security). In the proof, σ in the authenticator $\mathsf{cmd}_{\mathcal{S}}$ is omitted because it does not contribute to the security (it only contributes to the Full-ANO-CMA security).

First, we consider MAC.Auth as a public random function (Random Oracle) and introduce the so-called Primitive Oracle Prim. This returns $\mathsf{MAC.Auth}(\tilde{\mathsf{K}}, \tilde{\mathsf{m}})$ upon an input $(\tilde{\mathsf{K}}, \tilde{\mathsf{m}}) \in \mathcal{K} \times \mathcal{M}$. Then, we express the advantage of an adversary against UF-CMA security by that of a distinguisher D trying to distinguish the *real world* $(\mathsf{Auth}_o, \mathsf{Vrfy}_o, \mathsf{Corr}, \mathsf{Prim})$ and an *ideal world* $(\mathsf{Auth}_o, \mathsf{Rej}, \mathsf{Corr}, \mathsf{Prim})$. Auth_o oracle receives a query $(\mathsf{m}, \mathcal{S})$ and returns $\mathsf{Auth}(\mathsf{ak}, \mathsf{m}, \mathcal{S})$ as described at Sect. 2.6. Vrfy_o receives $(\mathsf{id}, \mathsf{cmd}_{\mathcal{S}})$ and returns $\mathsf{Vrfy}(\mathsf{vk}_{\mathsf{id}}, \mathsf{cmd}_{\mathcal{S}})$. Here, Rej oracle returns $\perp$ upon a verification query $(\mathsf{id}, \mathsf{cmd}_{\mathcal{S}} = (\mathsf{m}, x, \tau_{\sigma(1)}, \ldots, \tau_{\sigma(N)}))$ unless K_{id} has already been exposed by Corr, or $\mathsf{MAC.Auth}(\mathsf{K}_{\mathsf{id}}, \mathsf{m}||x)$ is included in an output section of Auth_o oracle for a query response to a recipient id; otherwise returns the correct value using K_{id} and a query history in Auth_o oracle. Let us assume that the number of queries to Auth_o are q_a and queries to Prim are q_p (queries to Corr do not specifically contribute to a success probability). Let

$$\phi_{\mathsf{Prim}} = ((\tilde{\mathsf{K}}_1, \tilde{\mathsf{m}}_1, \tilde{\tau}_1), \ldots, (\tilde{\mathsf{K}}_{q_p}, \tilde{\mathsf{m}}_{q_p}, \tilde{\tau}_{q_p}))$$

be the list of queries to Prim and corresponding answers. Let also

$$\phi_{\mathsf{Auth}} = ((\mathsf{m}_1, x_1, \tau_1), \ldots, (\mathsf{m}_{q_a}, x_{q_a}, \tau_{q_a}))$$

be the list of queries to Auth and corresponding answers.

We let

$$\phi_{\mathsf{Vrfy}} = (\mathsf{m}^*, \tau^*, b^*),$$

denote a query to Vrfy, where $b^* \in \{\top, \perp\}$. The tuple $\phi = (\phi_{\mathsf{Prim}}, \phi_{\mathsf{Auth}}, \phi_{\mathsf{Vrfy}}, \{\mathsf{K}_{\mathsf{id}}\}_{\mathsf{id} \in \mathcal{A}})$ forms the *transcript* of the attack, where $\mathcal{A}$ is a set of all identities involved in the game, namely those queried to Corr and those included in the queries to Auth_o and Vrfy_o. We assume that the subset of these keys not queried to Corr is attached to the script after the adversary made all queries (so that the adversary cannot use them to make further queries, which would trivially break any scheme); this is a common technique to simplify the proof. Also, we assume that all the keys are distributed uniformly for both worlds, that means, the keys those queried to Rej (and never queried to other oracles) in the ideal world are dummy

keys. We say that a transcript ϕ is *attainable* if the probability of getting this transcript in the ideal world is non-zero. We denote Φ as the set of attainable transcripts. We also let X_{Real}, X_{Ideal} denote the transcript random variable induced by the real world and the ideal world, respectively. Here, we say that an attainable transcript is *bad* if one of the following conditions holds:

1. There exists two distinct recipients $\mathsf{id}, \mathsf{id}'$ such that $\mathsf{K}_{\mathsf{id}} = \mathsf{K}_{\mathsf{id}'}$.
2. There exists a symmetric key $\tilde{\mathsf{K}}$ in a query $(\tilde{\mathsf{K}}, \tilde{\mathsf{m}})$ to Prim and a verification key K_{id} such that $(\tilde{\mathsf{K}} = \mathsf{K}_{\mathsf{id}})$.
3. A non-trivial forgery exists, i.e., $\phi_{\mathsf{Vrfy}} = (\mathsf{m}^*, \tau^*, b^*)$ with $b^* = \top$.

We denote Φ_{bad}, Φ_{good} as a set of bad transcripts and good transcripts, respectively.

Then, we will upper bound the advantage of the distinguisher by the H-coefficients technique:

Lemma 14 ([31]) *Let $\Phi = \Phi_{good} \cup \Phi_{bad}$ be a set of attainable transcripts. If there exists ϵ such that for any $\phi \in \Phi_{good}$, we have*

$$\frac{\Pr[X_{\mathsf{Real}} = \phi]}{\Pr[X_{\mathsf{Ideal}} = \phi]} \geq 1 - \epsilon,$$

and that there exists ϵ' such that $\Pr[X_{\mathsf{Ideal}} \in \Phi_{bad}] \leq \epsilon'$, the advantage of a distinguisher D then is upper bounded as $\mathsf{Adv}(\mathsf{D}) \leq \epsilon + \epsilon'$.

We now show a upper bound of the probability to get a bad transcript in the ideal world.

Lemma 15 *Let $t \leq N$ is the number of recipients appearing in a query to Auth or Vrfy. For any integers q_p,*

$$\Pr[X_{\mathsf{Ideal}} \in \Phi_{bad}] \leq \frac{(2t^2 + t \cdot q_p)}{|\mathcal{K}|}.$$

Proof First, we consider the condition 1. For verification keys $\mathsf{K}_{\mathsf{id}}, \mathsf{K}'_{\mathsf{id}}$, there are $\binom{t}{2}$ possible choices for $\mathsf{id}, \mathsf{id}'$. Then, the probability that the attainable transcript satisfy the condition is $\binom{t}{2}/|\mathcal{K}|$.

Next, we consider the condition 2. For each query to Prim, the distinguisher select a symmetric key $\tilde{\mathsf{K}}$ such that $\tilde{\mathsf{K}} = \mathsf{K}_{\mathsf{id}}$ for some id with probability $\frac{t}{|\mathcal{K}|}$. Thus, we can upper bound the probability that the condition 2 is satisfied by $\frac{t \cdot q_p}{|\mathcal{K}|}$. The condition 3 trivially never holds in the ideal world. From above we have

$$\begin{aligned}\Pr[X_{\mathsf{Ideal}} \in \Phi_{bad}] &\leq \frac{\binom{t}{2} + t \cdot q_p}{|\mathcal{K}|} \\ &\leq \frac{(2t^2 + t \cdot q_p)}{|\mathcal{K}|}.\end{aligned}$$

□

Lemma 16 *For any good transcript ϕ,*

$$\frac{\Pr[X_{\mathsf{Real}} = \phi]}{\Pr[X_{\mathsf{Ideal}} = \phi]} \geq 1 - \frac{N}{|\mathcal{T}|},$$

where $|\mathcal{S}| \leq N$.

Proof Let $\phi = (\phi_{\mathsf{Prim}}, \phi_{\mathsf{Auth}}, \phi_{\mathsf{Vrfy}}, \{\mathsf{K_{id}}\}_{\mathsf{id}\in\mathcal{A}})$ be a good transcript. When ϕ is good, the keys involved in the game has no non-trivial collisions, hence the outputs of Prim oracle are independent from other oracle responses except the trivial ones (those queried to both Prim and Corr). Moreover, all the responses from Auth_o are perfectly random except the trivial overlap of queried ids. This immediately implies that the probability ratio is the probability ratio for the event that Vrfy_o returns $\perp$ (i.e., $b^* = \perp$), since other variables in the transcript have identical distributions for the both worlds. In the ideal world, the probability of $b^* = \perp$ is one by definition. While in the real world, because the random oracle returns the completely random output for any distinct input, and the set of keys involved in the verification query must contain a distinct one from the definition of bad events and the game definition (that serves as the distinct input to the random oracle), the probability of $b^* = \perp$ is identical to the random guess of the true tag values. Hence it is at most $|\mathcal{S}|/|\mathcal{T}|$ when the verification query uses the id set $\mathcal{S}$. Therefore, we have

$$\frac{\Pr[X_{\mathsf{Real}} = \phi]}{\Pr[X_{\mathsf{Ideal}} = \phi]} = \frac{\Pr_{\mathsf{Real}}[b^* = \perp]}{\Pr_{\mathsf{Ideal}}[b^* = \perp]} \geq 1 - \frac{|\mathcal{S}|}{|\mathcal{T}|},$$

which proves Lemma 16. □

Proof of Theorem 8 For the UF-CMA secuity, by combining Lemmas 14, 15, and 16 we have

$$\mathsf{Adv}^{\mathsf{UF\text{-}CMA}}_{\Pi^{\mathsf{MAC}},\mathsf{A}}(\kappa) \leq \frac{(2t^2 + t \cdot q_p)}{|\mathcal{K}|} + \frac{1}{|\mathcal{T}|},$$

which concludes the proof.

Next, we now consider the Full-ANO-CMA security. Under the assumption that MAC.Auth is a public random function, when two kinds of key collisions does not occur (i.e. conditions 1 or 2 does not hold), the Full-ANO-CMA security can be proven since a set of recipients included in a symmetric difference ($\mathcal{S}_0 \triangle \mathcal{S}_1$) in a challenge query is completely unpredictable and a permutation σ is chosen completely at random for each challenge query. □

In addition, we can construct ABA that is UF-CMA secure and ANO-CMA secure by modifying the Auth and Vrfy algorithms in the above construction as follows:

- $\mathsf{Auth}(\mathsf{ak}, \mathsf{m}, \mathcal{S})$: Let n be the number of recipients currently participating in the system, and suppose that $\mathsf{vk_{id}}_1, \ldots, \mathsf{vk_{id}}_n$ have been generated by Join so far. Let $\mathsf{ak} = \{\mathsf{K_{id}}\}_{\mathsf{id}\in[N]}$, $x \xleftarrow{\cup} \mathcal{R}$, and compute $\tau \leftarrow \mathsf{MAC.Auth}(\mathsf{K_{id}}, \mathsf{m}||x)$ for all $\mathsf{id} \in \mathcal{S}$. Choose a random permutation σ from $\{\sigma_i : [|\mathcal{S}|] \to [|\mathcal{S}|]\}_{i\in\{0,1\}^\kappa}$ and the authenticator is
$$\mathsf{cmd}_{\mathcal{S}} := (\mathsf{m}, x, \tau_{\sigma(1)}, \ldots, \tau_{\sigma(|\mathcal{S}|)}).$$
- $\mathsf{Vrfy}(\mathsf{vk_{id}}, \mathsf{cmd}_{\mathcal{S}})$: Let $\mathsf{vk_{id}} = \mathsf{K_{id}}, \mathsf{cmd}_{\mathcal{S}} = (\mathsf{m}, x, \tau_1, \ldots, \tau_{|\mathcal{S}|})$. Do the following two steps from $j := 1$.
  - Run $\mathsf{MAC.Vrfy}(\mathsf{K_{id}}, \tau_j, \mathsf{m}||x)$ and if its output is $\top$, return m and halt; otherwise, go to the second step.
  - If $j = |\mathcal{S}|$, return $\perp$ and halt; otherwise, do the first step with $j := j + 1$.

Theorem 9 *Assume that* MAC.Auth *is a public random function. If* Π^{MAC} *is UF-CMA secure, the above construction is UF-CMA secure and ANO-CMA secure.*

Proof As in Theorem 8, we can prove that the above scheme meets the UF-CMA security. Also, the ANO-CMA security can be shown in a similar way to Theorem 8. Note that a

leakage of information about the number of designated recipients $\mathcal{S}$ does not involve the ANO-CMA security thanks to the condition $|\mathcal{S}_0| = |\mathcal{S}_1|$ in $\mathsf{Exp}^{\mathsf{ANO\text{-}CMA}}_{\Pi^{\mathsf{ABA}},\mathsf{A}}(\kappa, N)$ □

Here, by the same discussion as in Sect. 5, from the above constructions and the asymptotic lower bounds in Sect. 7, we show lower bounds on the authenticator-size in (Full)-ANO-BA.

Theorem 10 *If ABA Π^{ABA} with properties shown in Sects. 6.3 and 7 is Full-ANOat-CMA secure, a non-asymptotic lower bound on the authenticator-size with any recipient set $\mathcal{S} \subseteq \mathcal{ID}$ is $N \cdot \kappa + o(N \cdot \kappa)$, and our Full-ANO-BA scheme attains the lower bound tightly, which is optimal.*

Theorem 11 *If ABA Π^{ABA} with properties shown in Sects. 6.3 and 7 is ANOat-CMA secure, a non-asymptotic lower bound on the authenticator-size with any recipient set $\mathcal{S} \subseteq \mathcal{ID}$ is $|\mathcal{S}| \cdot \kappa + o(|\mathcal{S}| \cdot \kappa)$, and our ANO-BA scheme attains the lower bound tightly, which is optimal.*

9 Conclusion

We analyzed an efficiency limit of anonymous Broadcast Encryption (BE) which is a cryptosystem realizing a basic access control. Specifically, we derived an asymptotic lower bound on the ciphertext size in BE with anonymity (Anonymous BE), assuming only properties that most existing (Full-)ANO-BE schemes satisfy. Our lower bounds can be applied to the existing (Full-)ANO-BE schemes while Kiayias and Samari's ones [20] are hard to apply. As a result, we show that the existing ANO-BE schemes achieve the optimal ciphertext size. We further showed that our analysis can be extended to the authentication setting. Specifically, we first derived asymptotic lower bounds on the authenticator size required for anonymous broadcast authentication (ABA).

Furthermore, we extended the above result to derive non-asymptotic lower bounds on the ciphertext size in (Full-)ANO-BE, by proposing an optimal construction based on Li and Gong's ANO-BE scheme [24]. In addition, we applied the same analysis to ABA, and proposed an optimal construction of ABA to show non-asymptotic lower bounds on the authenticator size in ABA.

Acknowledgements We would like to thank Kyosuke Yamashita for pointing out the flaw in the proofs in the earlier version, and anonymous reviewers for insightful feedback. This research was conducted under a contract of "Research and development on IoT malware removal/make it non-functional technologies for effective use of the radio spectrum" among "Research and Development for Expansion of Radio Wave Resources (JPJ000254)," which was supported by the Ministry of Internal Affairs and Communications, Japan. This work was in part supported by JSPS KAKENHI Grant Numbers JP21H03395, JP22H03590.

Funding Open access funding provided by Yokohama National University.

Appendix A

In this section, we show that the BE scheme in [5] meets the properties defined in Sect. 3.2. We review Boneh et al's scheme.

BGW05 [5]

- $\mathsf{Setup}(1^\kappa, N)$: Run $\mathsf{PGGen}(1^\kappa)$ to get $\mathcal{PG} := (\mathsf{p}, \mathbb{G}, \mathbb{G}_T, \mathsf{e}, g)$. Let $\mathbb{Z}_p := \{1, \ldots, \mathsf{p}-1\}, \alpha, \mathsf{s} \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ and set $\mathsf{v} = \mathsf{g}^\mathsf{s}$. For all $\mathsf{id} = 1, 2, \ldots, N, N+2, \ldots, 2N$, compute $\mathsf{g}_\mathsf{id} = \mathsf{g}^{\alpha^\mathsf{id}}$. The public key is $\mathsf{pk} := \mathsf{g}, \mathsf{g}_1, \ldots, \mathsf{g}_n, \mathsf{g}_{N+2}, \ldots, \mathsf{g}_{2N}, \mathsf{v}$ and the master secret key is s.
- $\mathsf{Join}(\mathsf{mk}, \mathsf{id})$: Output the secret key $\mathsf{sk}_\mathsf{id} := (\mathsf{d}_\mathsf{id} = \mathsf{g}_\mathsf{id}^\mathsf{s}, \mathsf{pk})$.
- $\mathsf{Enc}(\mathsf{pk}, \mathsf{m}, \mathcal{S})$: Sample $r \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ and set $\mathsf{K} = \mathsf{e}(\mathsf{g}_{N+1}, \mathsf{g})^r$. Next, compute

$$\mathsf{ct}_\mathcal{S} := (\mathsf{g}^r, (\mathsf{v} \cdot \prod_{j \in \mathcal{S}} \mathsf{g}_{N+1-j})^r, \mathsf{K} \cdot \mathsf{m}, \mathcal{S})$$

  and output $\mathsf{ct}_\mathcal{S}$.
- $\mathsf{Dec}(\mathsf{sk}_\mathsf{id}, \mathsf{ct}_\mathcal{S})$: Let $\mathsf{sk}_\mathsf{id} = (\mathsf{d}_\mathsf{id} = \mathsf{g}_\mathsf{id}^\mathsf{s}, \mathsf{pk})$, $\mathsf{ct}_\mathcal{S} = (\mathsf{C}_0, \mathsf{C}_1, \mathsf{C}_2, \mathcal{S})$. Then output

$$\mathsf{m} = \frac{\mathsf{C}_2 \cdot \mathsf{e}\left(\mathsf{d}_\mathsf{id} \cdot \prod_{\substack{j \in \mathcal{S} \\ j \neq \mathsf{id}}} \mathsf{g}_{N+1-j+\mathsf{id}}, \mathsf{C}_0\right)}{\mathsf{e}\left(\mathsf{g}_\mathsf{id}, \mathsf{C}_1\right)}.$$

We show the correctness of the above scheme. We use the fact that $\mathsf{g}_i^{(\alpha_j)} = \mathsf{g}_{i+j}$ for any i, j. Suppose that $\mathsf{ct}_\mathcal{S} = (\mathsf{g}^r, (\mathsf{v} \cdot \prod_{j \in \mathcal{S}} \mathsf{g}_{N+1-j})^r, \mathsf{K} \cdot \mathsf{m}, \mathcal{S})$ are correctly generated. Then the following equation holds:

$$\begin{aligned}
\frac{\mathsf{e}\left(\mathsf{g}_\mathsf{id}, \mathsf{C}_1\right)}{\mathsf{e}\left(\mathsf{d}_\mathsf{id} \cdot \prod_{\substack{j \in \mathcal{S} \\ j \neq \mathsf{id}}} \mathsf{g}_{N+1-j+\mathsf{id}}, \mathsf{C}_0\right)} &= \frac{\mathsf{e}\left(\mathsf{g}^{(\alpha^\mathsf{id})}, (\mathsf{v} \cdot \prod_{j \in \mathcal{S}} \mathsf{g}_{N+1-j})^r\right)}{\mathsf{e}\left(\mathsf{v}^{(\alpha^\mathsf{id})} \cdot \prod_{\substack{j \in \mathcal{S} \\ j \neq \mathsf{id}}} \mathsf{g}_{N+1-j+\mathsf{id}}, \mathsf{g}^r\right)} \\
&= \frac{\mathsf{e}\left(\mathsf{g}^{(\alpha^\mathsf{id})}, (\mathsf{g}_{N+1-\mathsf{id}})^r\right) \cdot \mathsf{e}\left(\mathsf{g}^{(\alpha^\mathsf{id})}, (\mathsf{v} \cdot \prod_{\substack{j \in \mathcal{S} \\ j \neq \mathsf{id}}} \mathsf{g}_{N+1-j})^r\right)}{\mathsf{e}\left(\mathsf{v}^{(\alpha^\mathsf{id})} \cdot \prod_{\substack{j \in \mathcal{S} \\ j \neq \mathsf{id}}} \mathsf{g}_{N+1-j+\mathsf{id}}, \mathsf{g}^r\right)} \\
&= \frac{\mathsf{e}\left(\mathsf{g}_{N+1}, \mathsf{g}\right)^r \cdot \mathsf{e}\left(\mathsf{g}^{(\alpha^\mathsf{id})}, (\mathsf{v} \cdot \prod_{\substack{j \in \mathcal{S} \\ j \neq \mathsf{id}}} \mathsf{g}_{N+1-j})^r\right)}{\mathsf{e}\left(\mathsf{v}^{(\alpha^\mathsf{id})} \cdot \prod_{\substack{j \in \mathcal{S} \\ j \neq \mathsf{id}}} \mathsf{g}_{N+1-j+\mathsf{id}}, \mathsf{g}^r\right)}
\end{aligned}$$

$$
\begin{aligned}
&= \frac{\mathsf{e}\left(\mathsf{g}_{N+1}, \mathsf{g}\right)^{r} \cdot \mathsf{e}\left(\mathsf{g}, \left(\mathsf{v}^{(\alpha^{\mathsf{id}})} \cdot \prod_{\substack{j \in \mathcal{S} \\ j \neq \mathsf{id}}} \mathsf{g}_{N+1-j+\mathsf{id}}\right)^{r}\right)}{\mathsf{e}\left(\mathsf{v}^{(\alpha^{\mathsf{id}})} \cdot \prod_{\substack{j \in \mathcal{S} \\ j \neq \mathsf{id}}} \mathsf{g}_{N+1-j+\mathsf{id}}, \mathsf{g}^{r}\right)} \\
&= \mathsf{e}\left(\mathsf{g}_{N+1}, \mathsf{g}\right)^{r} \\
&= \mathsf{K}.
\end{aligned}
$$

Here, we can see the above scheme meets the properties. First, its public key, private key of a recipient $\mathsf{id} \in [N]$, and ciphertext with $\mathcal{S}$ can be described in AtBE's notation as follows: $\{\mathsf{pk}^{(\delta)}\}_{\delta \in \Delta} := \{\mathsf{g}, \mathsf{g}_1, \ldots, \mathsf{g}_N, \mathsf{g}_{N+2}, \ldots, \mathsf{g}_{2N}, \mathsf{v}\}$, $\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma \in \Gamma_{\mathsf{id}}} := \{\mathsf{g}_{\mathsf{id}}^{s}\} \cup \{\mathsf{pk}^{(\delta)}\}_{\delta \in \Delta}$, $\{\mathsf{ct}_{\mathcal{S}}^{(\theta)}\}_{\theta \in [\beta_{\mathcal{S}}]} = \mathsf{ct}_{\mathcal{S}} := \{(\mathsf{g}^{r}, (\mathsf{v} \cdot \prod_{j \in \mathcal{S}} \mathsf{g}_{N+1-j})^{r}), \mathsf{K} \cdot \mathsf{m}, \mathcal{S}\}$.

According to an atomic ciphertext, the following equations hold:

$$
\begin{aligned}
&\mathsf{ct}_{\mathcal{S},\mathsf{id}} := \{(\mathsf{g}^{r}, (\mathsf{v} \cdot \prod_{j \in \mathcal{S}} \mathsf{g}_{N+1-j})^{r}, \mathsf{K} \cdot \mathsf{m}, \mathcal{S})\}, \\
&\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma \in \Gamma'_{\mathsf{id}}} := \{\mathsf{g}_{\mathsf{id}}^{s}, \mathsf{g}, \{\mathsf{g}_{N+1-j+\mathsf{id}}\}_{\substack{j \in \mathcal{S} \\ j \neq \mathsf{id}}}, \mathsf{v}\}, \\
&\mathsf{m} \leftarrow \mathsf{Dec\text{-}at}(\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma \in \Gamma'_{\mathsf{id}}}, \mathsf{ct}_{\mathcal{S},\mathsf{id}}).
\end{aligned}
$$

where Dec-at corresponds to Dec algorithm in BGW05 scheme. Hence, Property 1 is satisfied.

According to a public key, a minimum subset of atomic public keys used to generate $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$ is uniquely determined as $\{\mathsf{pk}^{(\delta)}\}_{\delta \in \Delta^{*}_{\mathsf{id},\mathcal{S},\mathsf{m}}} := \{\mathsf{g}, \{\mathsf{g}_{N+1-j}\}_{j \in \mathcal{S}}, \mathsf{v}\}$. Therefore, Property 2 is met.

According to a decryption key, a minimum subset of atomic decryption keys used to decrypt $\mathsf{ct}_{\mathcal{S},\mathsf{id}}$, is uniquely determined as $\{\mathsf{sk}_{\mathsf{id}}^{(\gamma)}\}_{\gamma \in \Gamma^{*}_{\mathsf{id},\mathcal{S}}} := \{\mathsf{g}_{\mathsf{id}}^{s}, \mathsf{g}, \{\mathsf{g}_{N+1-j+\mathsf{id}}\}_{\substack{j \in \mathcal{S} \\ j \neq \mathsf{id}}}, \mathsf{v}\}$. Therefore, Property 3 is satisfied.

An atomic ciphertext with id' is given as $\mathsf{ct}_{\mathcal{S},\mathsf{id}'} := \{(\mathsf{g}^{r}, (\mathsf{v} \cdot \prod_{j \in \mathcal{S}} \mathsf{g}_{N+1-j})^{r}), \mathsf{K} \cdot \mathsf{m}, \mathcal{S}\}$, and if $\mathsf{ct}_{\mathcal{S},\mathsf{id}} = \mathsf{ct}_{\mathcal{S},\mathsf{id}'}$ holds, then we have $\{\mathsf{pk}^{(\delta)}\}_{\delta \in \Delta^{*}_{\mathsf{id},\mathcal{S},\mathsf{m}}} = \{\mathsf{pk}^{(\delta')}\}_{\delta' \in \Delta^{*}_{\mathsf{id}',\mathcal{S},\mathsf{m}}}$ with overwhelming probability. Therefore, Property 4 is also satisfied.

From the above, we can see that the BE scheme in [5] meets Properties 1, 2, 3 and 4. In addition, we can similarly show that the existing (both non-anonymous and anonymous) BE schemes [1–3, 6, 15, 16, 24, 25, 30, 38] satisfy Properties 1, 2, 3 and 4 as well, thus it is reasonable to assume Properties 1, 2, 3 and 4 in this paper.

We also show that the ANO-BE scheme in [25] has the property in Assumption 2 defined in Sect. 4.1. We review Libert et al's Full-ANO-BE scheme [25].

LPQ12 [25]

- $\mathsf{Setup}(1^{\kappa}, N)$: Let $\mathsf{PKE} := (\mathsf{PKE.KGen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ be a PKE scheme with message space $\mathcal{M} = \{0,1\}^{m}$ and $\mathsf{OTS} := (\mathsf{OTS.KGen}, \mathsf{OTS.Sign}, \mathsf{OTS.Vrfy})$ be an one-time signature scheme with key space $\mathcal{SK} = \{0,1\}^{v}$, for some $v \in \mathsf{poly}(1^{\kappa})$. For all $\mathsf{id} \in [N]$, run $(\mathsf{pke.pk}_{\mathsf{id}}, \mathsf{pke.sk}_{\mathsf{id}}) \leftarrow \mathsf{PKE.KGen}(1^{\kappa})$. The public key pk is

$$\left(\left\{\mathsf{pke.pk}_{\mathsf{id}}\right\}_{\mathsf{id}=1}^{N}, \mathsf{OTS}, 1^{\kappa}\right).$$

and the master secret key is $\{\mathsf{pke.sk}_{\mathsf{id}}\}_{\mathsf{id}=1}^{N}$, where OTS is

- $\mathsf{Join}(\mathsf{mk}, \mathsf{id})$: Output the secret key $\mathsf{sk}_{\mathsf{id}} := \mathsf{pke.sk}_{\mathsf{id}}$.
- $\mathsf{Enc}(\mathsf{pk}, \mathsf{m}, \mathcal{S})$: Let n be the number of recipients currently participating in the system, and suppose that $\mathsf{sk}_{\mathsf{id}_1}, \ldots, \mathsf{sk}_{\mathsf{id}_n}$ have been generated by Join so far. Compute the following for all $\mathsf{id} \in [N]$:

$$\begin{cases} \mathsf{pke.ct}_{\mathsf{id}} \leftarrow \mathsf{PKE.Enc}(\mathsf{pke.pk}_{\mathsf{id}}, \mathsf{m}||\mathsf{ots.vk}), \text{ if } \mathsf{id} \in \mathcal{S}, \\ \mathsf{pke.ct}_{\mathsf{id}} \leftarrow \mathsf{PKE.Enc}(\mathsf{pke.pk}_{\mathsf{id}}, 0^v||\mathsf{ots.vk}), \text{ if } \mathsf{id} \notin \mathcal{S}. \end{cases}$$

  Run $(\mathsf{ots.sk}, \mathsf{ots.vk}) \leftarrow \mathsf{OTS.KGen}(1^\kappa)$. Choose a random permutation σ from $\{\sigma_i : [N] \to [N]\}_{i \in \{0,1\}^\kappa}$ and run $\sigma \leftarrow \mathsf{OTS.Sign}(\mathsf{ots.sk}, \{\mathsf{pke.ct}_{\mathsf{id}}\}_{\mathsf{id}=1}^N)$. The ciphertext is

$$\mathsf{ct}_{\mathcal{S}} := (\mathsf{pke.ct}_{\sigma(1)}, \ldots, \mathsf{pke.ct}_{\sigma(N)}, \sigma).$$

- $\mathsf{Dec}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct}_{\mathcal{S}})$: Let $\mathsf{sk}_{\mathsf{id}} = \mathsf{pke.sk}_{\mathsf{id}}$, $\mathsf{ct}_{\mathcal{S}} = (\sigma, \mathsf{pke.ct}_1, \ldots, \mathsf{pke.ct}_N)$. Do the following two steps from $j := 1$.
  - Compute $\mathsf{m}' \leftarrow \mathsf{PKE.Dec}(\mathsf{pke.sk}_{\mathsf{id}}, \mathsf{pke.ct}_j)$ and parse m' as $\mathsf{m}||\mathsf{ots.vk}$ for some bit-strings $\mathsf{m} \in \{0,1\}^{m-v}$ and $\mathsf{ots.vk} \in \{0,1\}^v$. Then, if $\mathsf{OTS.Vrfy}(\mathsf{ots.vk}, (\mathsf{pke.ct}_1, \ldots, \mathsf{pke.ct}_N), \sigma) \to 1$ and $\mathsf{m}' \notin \{0^v, \perp\}$, return m and halt; otherwise, go to the second step.
  - If $j = N$, return $\perp$ and halt; otherwise, do the first step with $j := j + 1$.

The correctness of the above scheme follows directly from the correctness of PKE and OTS.

In the above scheme, PKE.Enc executed inside Enc corresponds to Enc-at, and PKE.Dec executed inside Dec corresponds to Dec-at. Then, $\mathcal{PK}^*$ and $\mathcal{SK}^*$ indicates $\{\mathsf{pke.pk}_{\mathsf{id}}\}_{\mathsf{id} \in [N]}$ and $\{\{\mathsf{pke.sk}_1\}, \ldots, \{\mathsf{pke.sk}_N\}\}$ respectively, and $\mathsf{pke.sk}_{\mathsf{id}} = \mathsf{sk}'$ such that $\mathsf{m}' \leftarrow \mathsf{PKE.Dec}(\mathsf{pke.sk}_{\mathsf{id}}, \mathsf{ct}_{\mathcal{S},\mathsf{id}})$ is uniquely determined by $\mathsf{pke.pk}_{\mathsf{id}} \in 2^{\mathcal{PK}^*}$. Therefore, Libert et al.'s scheme satisfies the property in Assumption 2.

References

1. Agrawal S., Yamada S.: Optimal broadcast encryption from pairings and LWE. In: Canteaut A., Ishai Y. (eds.) Advances in Cryptology—EUROCRYPT 2020, pp. 13–43. Springer, Cham (2020).
2. Agrawal S., Wichs D., Yamada S.: Optimal broadcast encryption from LWE and pairings in the standard model. In: Pass R., Pietrzak K. (eds.) Theory of Cryptography, pp. 149–178. Springer, Cham (2020).
3. Barth A., Boneh D., Waters B.: Privacy in encrypted content distribution using private broadcast encryption. In: Di Crescenzo G., Rubin A. (eds.) Financial Cryptography and Data Security, pp. 52–64. Springer, Berlin (2006).
4. Blazy O., Kiltz E., Pan J.: (hierarchical) Identity-based encryption from affine message authentication. In: Garay J.A., Gennaro R. (eds.) Advances in Cryptology—CRYPTO 2014, pp. 408–425. Springer, Berlin (2014).
5. Boneh D., Gentry C., Waters B.: Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Shoup V. (ed.) Advances in Cryptology—CRYPTO 2005, pp. 258–275. Springer, Berlin (2005).
6. Boneh D., Waters B., Zhandry M.: Low overhead broadcast encryption from multilinear maps. In: Garay J.A., Gennaro R. (eds.) Advances in Cryptology—CRYPTO 2014, pp. 206–223. Springer, Berlin (2014).
7. Chan H., Perrig A.: Round-efficient broadcast authentication protocols for fixed topology classes, pp. 257–272 (2010). https://doi.org/10.1109/SP.2010.22.
8. Cogliati B., Lee J., Seurin Y.: New constructions of macs from (tweakable) block ciphers. IACR Trans. Symmetric Cryptol. **2017**(2), 27–58 (2017). https://doi.org/10.13154/tosc.v2017.i2.27-58.
9. Escala A., Herold G., Kiltz E., Ràfols C., Villar J.: An algebraic framework for Diffie-Hellman assumptions. In: Canetti R., Garay J.A. (eds.) Advances in Cryptology—CRYPTO 2013, pp. 129–147. Springer, Berlin (2013).

10. Fazio N., Perera I.M.: Outsider-anonymous broadcast encryption with sublinear ciphertexts. In: Fischlin M., Buchmann J., Manulis M. (eds.) Public Key Cryptography—PKC 2012, pp. 225–242. Springer, Berlin (2012).
11. Fiat A., Naor M.: Broadcast encryption. In: Stinson D.R. (ed.) Advances in Cryptology—CRYPTO' 93, pp. 480–491. Springer, Berlin (1994).
12. Fischlin M.: Pseudorandom function tribe ensembles based on one-way permutations: improvements and applications. In: EUROCRYPT (1999).
13. Gay R., Hofheinz D., Kiltz E., Wee H.: Tightly CCA-secure encryption without pairings. In: Fischlin M., Coron J.-S. (eds.) Advances in Cryptology—EUROCRYPT 2016, pp. 1–27. Springer, Berlin (2016).
14. Gay R., Hofheinz D., Kohl L.: Kurosawa-Desmedt meets tight security. In: Katz J., Shacham H. (eds.) Advances in Cryptology—CRYPTO 2017, pp. 133–160. Springer, Cham (2017).
15. Gay R., Kowalczyk L., Wee H.: Tight adaptively secure broadcast encryption with short ciphertexts and keys. In: Catalano D., De Prisco R. (eds.) Security and Cryptography for Networks, SCN 2018, pp. 123–139. Springer, Cham (2018).
16. Gentry C., Waters B.: Adaptive security in broadcast encryption systems (with short ciphertexts). In: Joux A. (ed.) Advances in Cryptology—EUROCRYPT 2009, pp. 171–188. Springer, Berlin (2009).
17. Han S., Liu S., Qin B., Gu D.: Tightly CCA-secure identity-based encryption with ciphertext pseudorandomness. Des. Codes Cryptogr. **86**, 517–554 (2018). https://doi.org/10.1007/s10623-017-0339-3.
18. Hofheinz D.: Adaptive partitioning. In: Coron J.-S., Nielsen J.B. (eds.) Advances in Cryptology—EUROCRYPT 2017, pp. 489–518. Springer, Cham (2017).
19. Hofheinz D., Jia D., Pan J.: Identity-based encryption tightly secure under chosen-ciphertext attacks. In: Peyrin T., Galbraith S. (eds.) Advances in Cryptology—ASIACRYPT 2018, pp. 190–220. Springer, Cham (2018).
20. Kiayias A., Samari K.: Lower bounds for private broadcast encryption. In: Kirchner M., Ghosal D. (eds.) Information Hiding, pp. 176–190. Springer, Berlin (2013).
21. Kiltz E., Wee H.: Quasi-adaptive NIZK for linear subspaces revisited. In: Oswald E., Fischlin M. (eds.) Advances in Cryptology—EUROCRYPT 2015, pp. 101–128. Springer, Berlin (2015).
22. Kobayashi H., Watanabe Y., Shikata J.: Asymptotically tight lower bounds in anonymous broadcast encryption and authentication. In: Paterson M.B. (ed.) Cryptography and Coding, pp. 105–128. Springer, Cham (2021).
23. Langrehr R., Pan J.: Tightly secure hierarchical identity-based encryption. J. Cryptol. **33**(4), 1787–1821 (2020).
24. Li J., Gong J.: Improved anonymous broadcast encryptions. In: Preneel B., Vercauteren F. (eds.) Applied Cryptography and Network Security, ACNS 2018, pp. 497–515. Springer, Cham (2018).
25. Libert B., Paterson K.G., Quaglia E.A.: Anonymous broadcast encryption: adaptive security and efficient constructions in the standard model. In: Fischlin M., Buchmann J., Manulis M. (eds.) Public Key Cryptography—PKC 2012, pp. 206–224. Springer, Berlin (2012).
26. Lyu L., Liu S., Han S., Gu D.: Tightly sim-so-CCA secure public key encryption from standard assumptions. In: Abdalla M., Dahab R. (eds.) Public-Key Cryptography—PKC 2018, pp. 62–92. Springer, Cham (2018).
27. Mandal M., Nuida K.: Identity-based outsider anonymous broadcast encryption with simultaneous individual messaging. In: Kutyłowski M., Zhang J., Chen C. (eds.) Network and System Security, pp. 167–186. Springer, Cham (2020).
28. Morgan A., Pass R., Shi E.: On the adaptive security of MACS and PRFS. In: Moriai S., Wang H. (eds.) Advances in Cryptology—ASIACRYPT 2020, pp. 724–753. Springer, Cham (2020).
29. Morillo P., Ràfols C., Villar J.L.: The kernel matrix Diffie-Hellman assumption. In: Cheon J.H., Takagi T. (eds.) Advances in Cryptology—ASIACRYPT 2016, pp. 729–758. Springer, Berlin (2016).
30. Naor D., Naor M., Lotspiech J.: Revocation and tracing schemes for stateless receivers. In: Kilian J. (ed.) Advances in Cryptology—CRYPTO 2001, pp. 41–62. Springer, Berlin (2001).
31. Patarin J.: The coefficients h technique. In: Avanzi R.M., Keliher L., Sica F. (eds.) Selected Areas in Cryptography, pp. 328–345. Springer, Berlin (2009).
32. Perrig A.: The biba one-time signature and broadcast authentication protocol. In: Proc. 8th ACM Conference on Computer and Communications Security, pp. 28–37 (2001).
33. Perrig A., Canetti R., Tygar J.D., Song D.X.: Efficient authentication and signing of multicast streams over lossy channels. In: Proceedings of 2000 TEEE Symposium on Security and Privacy. S&P, pp. 56–73 (2000).
34. Perrig A., Canetti R., Tygar J.D., Song D.: TESLA: Multicast source authentication transform. IETF draft. draft-ietf-msec-tesla-intro-03.txt (2004).
35. Rivest R.L., Shamir A., Tauman Y.: How to leak a secret. In: Boyd C. (ed.) Advances in Cryptology—ASIACRYPT 2001, pp. 552–565. Springer, Berlin (2001).

36. Shoup V.: Sequences of games: a tool for taming complexity in security proofs. In: IACR Cryptology ePrint Archive 2004, p. 332 (2004).
37. Watanabe Y., Yanai N., Shikata J.: Anonymous broadcast authentication for securely remote-controlling IoT devices. In: Barolli L., Woungang I., Enokido T. (eds.) Advanced Information Networking and Applications, pp. 679–690. Springer, Cham (2021).
38. Waters B.: Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions. In: Halevi S. (ed.) Advances in Cryptology—CRYPTO 2009, pp. 619–636. Springer, Berlin (2009).
39. Wee H.: Déjà q: Encore! un petit ibe. In: Kushilevitz E., Malkin T. (eds.) Theory of Cryptography, pp. 237–258. Springer, Berlin (2016).
40. Zhang L., Wu Q., Mu Y.: Anonymous identity-based broadcast encryption with adaptive security. In: Wang G., Ray I., Feng D., Rajarajan M. (eds.) Cyberspace Safety and Security, pp. 258–271. Springer, Cham (2013).