Improved Anonymous Broadcast Encryptions

Tight Security and Shorter Ciphertext

Jiangtao Li[1] and Junqing Gong[2](✉)

[1] East China Normal University, Shanghai, China
lijiangtao@stu.ecnu.edu.cn
[2] ENS de Lyon, Laboratoire LIP (U. Lyon, CNRS, ENSL, INRIA, UCBL), Lyon, France
junqing.gong@ens-lyon.fr

Abstract. We investigate anonymous broadcast encryptions (ANOBE) in which a ciphertext hides not only the message but also the target recipients associated with it. Following Libert *et al.*'s generic construction [PKC, 2012], we propose two concrete ANOBE schemes with tight reduction and better space efficiency.

- The IND-CCA security and anonymity of our two ANOBE schemes can be tightly reduced to standard k-Linear assumption (and the existence of other primitives). For a broadcast system with n users, Libert *et al.*'s security analysis suffers from $O(n^3)$ loss while our security loss is constant.
- Our first ANOBE supports fast decryption and has a shorter ciphertext than the fast-decryption version of Libert *et al.*'s concrete ANOBE. Our second ANOBE is adapted from the first one. We sacrifice the fast decryption feature and achieve shorter ciphertexts than Libert *et al.*'s concrete ANOBE with the help of bilinear groups.

Technically, we start from an instantiation of Libert *et al.*'s generic ANOBE [PKC, 2012], but we work out all our proofs from scratch instead of relying on their generic security result. This intuitively allows our optimizations in the concrete setting.

Keywords: Broadcast encryption · Full anonymity
Chosen-ciphertext security · Tight reduction · Short ciphertext

1 Introduction

Broadcast Encryption. *Broadcast encryption* [Ber91,FN94] (BE) is a public-key cryptosystem designed for securely sending information to multiple users via

J. Li—Shanghai Key Laboratory of Trustworthy Computing, School of Computer Science and Software Engineering. Supported by the National Key R&D program of China (No. 2017YFB0802000) and NSF of China (Nos. 61572198, 61632012, 61672239). Part of this work was done while the author was visiting ENS de Lyon.
J. Gong—Supported by the French ANR ALAMBIC project (ANR-16-CE39-0006).

B. Preneel and F. Vercauteren (Eds.): ACNS 2018, LNCS 10892, pp. 497–515, 2018.
https://doi.org/10.1007/978-3-319-93387-0_26

a public channel. In a BE system, we may index each user by integers $1, \ldots, n$ and name set $U := \{1, \ldots, n\}$ the *universe*. It would be convenient to describe BE in the framework of *Functional Encryption* [BSW11]. An authority publishes a set of public parameters generated by the Setup algorithm. Each user's secret key is then created by the KeyGen algorithm from the master secret key which is the output of Setup. By invoking the encryption algorithm Enc, a sender can create a ciphertext for users specified by a target set $S \subseteq U$. Any user with an index $i \in S$ is able to decrypt the ciphertext using the Dec algorithm.

The basic security requirement is *collusion-resistance* which ensures that a ciphertext leaks no information about the message even when multiple users outside the target set S decide to cooperate. More formally, it is required that

$$\{\mathsf{ct} \leftarrow_{\mathrm{R}} \mathsf{Enc}(\mathsf{mpk}, S, m_0)\} \approx_c \{\mathsf{ct} \leftarrow_{\mathrm{R}} \mathsf{Enc}(\mathsf{mpk}, S, m_1)\}$$

where mpk is the public parameters, $(S \subseteq U, m_0, m_1)$ are chosen by the adversary; and we allow the adversary to adaptively learn secret keys for all $i \notin S$.

With more powerful functional encryptions such as attribute-based encryptions [SW05, GPSW06, OT10, LOS+10, CGW15], we can securely broadcast information in a structural way which is more efficient and much easier to manage. However the classical BE still serves as the most general tool for broadcasting information in the systems where users are not well-organized, e.g., a country-wide pay-TV system.

Anonymity. Since been introduced, a series of BE schemes have been published [FN94, NNL01, YFDL04, BGW05, DPP07, GW09, Wee16], but they only ensure the confidentiality of the message while the target set S is entirely exposed to the public. In fact, the description of S will be directly transmitted through the insecure channel for decryption. However in many applications, the confidentiality of the target set is also crucial. For instance, in the pay-TV setting, everyone has access to the full list of subscribers, which is not acceptable. Therefore, it is desirable and non-trivial to build a BE system taking both the message and the target set into account in terms of confidentiality. In this paper, we call the latter feature *anonymity* and name such a BE as *anonymous broadcast encryption* [LPQ12] (ANOBE). More formally, it is required that

$$\{\mathsf{ct} \leftarrow_{\mathrm{R}} \mathsf{Enc}(\mathsf{mpk}, S_0, m_0)\} \approx_c \{\mathsf{ct} \leftarrow_{\mathrm{R}} \mathsf{Enc}(\mathsf{mpk}, S_1, m_1)\}$$

where (m_0, m_1, S_0, S_1) are chosen by the adversary and secret keys for all $i \notin (S_0 \setminus S_1) \cup (S_1 \setminus S_0)$ can be revealed. The subtlety is that any secret key for $i \in S_0 \cap S_1$ will give an adversary the power to correctly decrypt both ciphertexts above. In this case, $m_0 \neq m_1$ is disallowed in order to avoid the trivial attack.

State of the Art. Although anonymity is crucial for BE, it has not received much attentions to construct ANOBE with the proper security guarantee.

In 2006, Barth *et al.* [BBW06] first identified the *anonymity* (i.e., *recipient privacy* in their work) in the context of encrypted file system. They introduced the notion of ANOBE in the name of *private broadcast encryption*. In their work, two constructions were described. The first one is a generic construction from an IND-CCA secure PKE with key-privacy and a strongly unforgeable signature scheme. They claimed that it achieves IND-CCA security and anonymity but in the *selective* (or static) model which means that the adversary must commit the challenge target sets (S_0, S_1) in advance. Basically, a BE ciphertext there is a set of PKE ciphertexts intended for every recipient in S bound together via a signature. One drawback of this construction is that the decryption time is proportional to $|S|$ since each receiver has to try to decrypt each PKE ciphertext one by one. In their second construction, they introduced a method helping a receiver to find the right PKE ciphertext and reduced the decryption cost to constant. However, it unfortunately relies on the random oracle model.

At PKC 2012, Libert *et al.* [LPQ12] formally revisited Barth *et al.*'s results. They described the *adaptive* security for ANOBE where the adversary can choose the challenge target sets (S_0, S_1) at any time (i.e., the security notation we have reviewed), and showed that it can be achieved from IND-CCA secure PKE (plus strongly secure signatures). Note that this result is quite strong in that the underlying PKE is not necessarily key-private. Moreover, the receiver can decrypt in a constant time. However, the size of ciphertext depends on n, the size of universe. They then demonstrated that Barth *et al.*'s first BE is actually IND-CCA secure and anonymous in an *adaptive* sense and provided an alternative construction from IBE [Sha84, CHK04]. This ANOBE has shorter ciphertext (of size $O(|S|)$) but requires the underlying PKE to be weakly robust [ABN10, Moh10] and key-private, and the decryption cost increases to $O(|S|)$. They also formalized the method helping to reduce the decryption cost in Barth *et al.*'s second construction [BBW06] as *anonymous hint system*, which can be viewed as a variant of extractable hash proof systems [Wee10]. The classical randomness-reuse technique [Kur02, BBS03] was then formally studied to reduce the ciphertext size. Finally, a concrete ANOBE based on the Kurosawa-Desmedt PKE [KD04] was proposed. Having their generic ANOBE, they showed that the Kurosawa-Desmedt PKE can be adapted to be key-private and robust, and also support randomness-reuse technique.

Also at PKC 2012, Fazio and Perera [FP12] proposed an ANOBE scheme with sublinear-size ciphertexts but with a much weaker *outsider-anonymity* where users identified by $S_0 \cap S_1$ are not considered to be malicious. More formally, the adversary is forbidden to get any secret key for $i \in S_0 \cap S_1$. However Barth *et al.*'s early work [BBW06] has actually recognized such an inside attacker as a hazard and illustrated how serious the issue is under a chosen-ciphertext attack. In the end, we want to note that Libert *et al.*'s results [LPQ12] are still the best in the sense that they achieve (1) IND-CCA security, (2) *fully* anonymity and (3) random-oracle-freeness. To our best knowledge, there is no follow-up result with all these features simultaneously even when taking the *identity-based* variant into account (see recent work [HWL+16] for more details).

1.1 Contributions

In this paper, we propose two concrete ANOBE schemes. Both of them are obtained by optimizing an instantiation of Libert *et al.*'s generic construction [LPQ12] with *Cramer-Shoup PKE* [CS98,CS02]. We prove, *from scratch*, that they are secure in the sense of [LPQ12] from the standard k-Linear (k-Lin) assumption and the existence of several other cryptographic primitives (such as strongly unforgeable signature and collision-resistant hash function).

Although our proposals do not deviate from Libert *et al.*'s generic framework [LPQ12], our new start point and customized security proof allow us to gain shorter ciphertexts and tighter reduction than the concrete instantiation in [LPQ12]. (Recall that it is based on Kurosawa-Desmedt PKE [KD04] and the security result follows the generic construction directly.) A comparison between them is shown in Table 1 where we consider instantiations of our two ANOBE under DDH = 1-Lin (or SXDH = 1-Lin) assumption[1]. We note that these two instantiations are the most efficient ones.

Table 1. Comparison of our two proposals and the concrete ANOBE from [LPQ12] in terms of ciphertext size and reduction tightness. Table (a) is for the schemes supporting fast decryption while we tolerate linear decryption cost in Table (b). In our comparison, the system has n users and ℓ is the size of target set S. We let $\mathbb{G}$ be a finite group where DDH holds while $\mathbb{G}_1$ denotes the first source group of a bilinear group where SXDH holds. The column "Reduction" shows the security loss.

(a) Comparing our first ANOBE with [LPQ12] plus anonymous hint system.

Scheme	$\lvert\mathsf{ct}\rvert$	Reduction
[LPQ12]	$(4\ell+5)\lvert\mathbb{G}\rvert+2\lvert\mathbb{Z}_p\rvert$	$O(n^3)$
Sect. 3	$(2\ell+5)\lvert\mathbb{G}\rvert+2\lvert\mathbb{Z}_p\rvert$	$O(1)$

(b) Comparing our second ANOBE with [LPQ12] *without* anonymous hint system.

Scheme	$\lvert\mathsf{ct}\rvert$	Reduction
[LPQ12]	$(2\ell+5)\lvert\mathbb{G}\rvert+2\lvert\mathbb{Z}_p\rvert$	$O(n^3)$
Sect. 4	$(\ell+6)\lvert\mathbb{G}_1\rvert$	$O(1)$

Shorter Ciphertext. Our first ANOBE scheme supports fast decryption. Compared with the concrete ANOBE in [LPQ12] equipped with their DDH-based anonymous hint system[2], our ANOBE can save roughly 50% bandwidth. Our second ANOBE is derived from the first one. We sacrifice fast decryption and peruse shorter ciphertext. Compared with concrete ANOBE in [LPQ12], our second ANOBE works with bilinear groups and roughly saves 50% bandwidth[3]. We highlight that this construction almost touches the lower bound of ciphertext size in an anonymous broadcast encryption [KS12]. It is quite surprising that we start from a less efficient basic PKE scheme but finally achieves better space efficiency. We note that the Cramer-Shoup PKE [CS98,CS02] is indeed

[1] We assume that (1) the verification key and signature for strongly unforgeable one-time signatures consist of 3 group elements and 2 integers, respectively [Gro06] (see Sect. 4, [CCS09]); (2) the authenticated encryption with key-binding property has a ciphertext of roughly 2 group elements (see Sect. 6, [LPQ12]).

[2] The resulting ANOBE will also support fast decryption, here we share the randomness between ANOBE and anonymous hint system.

[3] Here we implement the concrete ANOBE from [LPQ12] using elliptic curve.

less efficient than Kurosawa-Desmedt PKE [KD04], but it permits us to use some customized method to optimize the system.

Tighter Reduction. In [LPQ12], their security reduction suffers from $O(n^3)$ loss where n is the size of the universe. This makes it infeasible for large-scale systems such as aforementioned pay-TV application. In particular, we need to use a larger group to compensate the loss, which of course increases the bandwidth and computation costs. In our work, we prove the security of two ANOBE from basic assumption and only suffer constant security loss, which is of both theoretical and practical interest. We argue that the result is non-trivial: A potential solution is to employ an IND-CCA secure PKE with tight reduction for multiple users (like [GHKW16,Hof17]) in Libert *et al.*'s generic construction [LPQ12]. However, the simulator still needs to guess which public keys will be associated with target set which is chosen adversarially and causes significant security loss.

1.2 Technical Overview

Our starting point is an instantiation of Libert *et al.*'s generic construction with Cramer-Shoup PKE [CS98,CS02]. In this overview, we first give this instantiation and describe how to derive our two ANOBE schemes from it.

Starting Point. Assume a *prime-order group* $(p, \mathbb{G}, g)$. We let $[a] := g^a \in \mathbb{G}$ for all $a \in \mathbb{Z}_p$ and extend it to matrix over $\mathbb{Z}_p$. Assume $S := \{i_1, \ldots, i_\ell\}$. We can instantiate Libert *et al.*'s construction using Cramer-Shoup PKE under k-Lin assumption as below:

$$\begin{aligned} \mathsf{mpk} &: \{\, [\mathbf{A}]\,, [\mathbf{A}^\top \mathbf{k}_i], [\mathbf{A}^\top \mathbf{x}_i], [\mathbf{A}^\top \mathbf{y}_i]\,\}_{i \in [n]}, (\mathsf{Gen}_{\mathsf{ots}}, \mathsf{Sig}, \mathsf{Ver}), \mathsf{h} \\ \mathsf{sk}_i &: \mathbf{k}_i, \mathbf{x}_i, \mathbf{y}_i \\ \mathsf{ct}_S &: \{\, [\mathbf{r}^\top \mathbf{A}^\top]\,, [\mathbf{r}^\top \mathbf{A}^\top \mathbf{k}_{i_j}] \cdot m, [\mathbf{r}^\top \mathbf{A}^\top (\mathbf{x}_{i_j} + \alpha \cdot \mathbf{y}_{i_j})]\,\}_{j \in [\ell]}, \mathsf{pk}_{\mathsf{ots}}, \sigma \end{aligned}$$

where $\mathbf{A} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{(k+1)\times k}$, $\mathbf{k}_i, \mathbf{x}_i, \mathbf{y}_i \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}$ for $i \in [n]$ and $\mathbf{r} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$. The public parameter mpk is basically n public keys of Cramer-Shoup PKE[4] sharing $[\mathbf{A}]$ which is a common technique in the multi-user setting. The ciphertext for S contains ℓ ciphertexts of Cramer-Shoup PKE with randomness $[\mathbf{r}^\top \mathbf{A}^\top]$ reused as [LPQ12]. Following Libert *et al.*'s suggestion, they are then bound together via a strongly unforgeable signature σ under fresh verification key $\mathsf{pk}_{\mathsf{ots}}$ instead of encrypting $m||\mathsf{pk}_{\mathsf{ots}}$.

The above BE is IND-CCA secure and anonymous according to Libert *et al.*'s generic result. However, we can do better by showing a tighter reduction for this concrete ANOBE. The security loss of Libert *et al.*'s reduction (which is $O(n^3)$) is mainly caused by black-box-reduction to the underlying PKE where the simulation need to guess some information about challenge target set. We prove our security result *from scratch*. In particular, we employ the proof technique for

[4] Here we use a direct generalization of Cramer-Shoup PKE under the k-Lin assumption. The original Cramer-Shoup PKE corresponds to the case $k = 1$.

IND-CCA PKE in the multi-user setting [GHKW16,Hof17] but adapt it to our broadcast encryption case. We found that we can now avoid guessing adversary's behavior and also corresponding reduction loss.

Our First ANOBE: Shorter Ciphertext for Fast Decryption. The above instantiation has not been equipped with anonymous hint system [LPQ12], so the decryption cost should be $O(\ell)$. (Recall that, intuitively, an anonymous hint system can help the decryptor to find the right ciphertext component intended for him and avoid $O(\ell)$ factor.) However we observe that $\{[\mathbf{r}^\top \mathbf{A}^\top(\mathbf{x}_{i_j} + \alpha \cdot \mathbf{y}_{i_j})]\}_{j\in[\ell]}$ can serve as the hints for fast decryption. This benefits from the fact that tag α is shared by all users in S. In the decryption procedure, a user with secret key $\mathbf{k}_i, \mathbf{x}_i, \mathbf{y}_i$ can recover $v = [\mathbf{r}^\top \mathbf{A}^\top(\mathbf{x}_i + \alpha \cdot \mathbf{y}_i)]$ and try to find the index j^* such that $v = [\mathbf{r}^\top \mathbf{A}^\top(\mathbf{x}_{i_{j^*}} + \alpha \cdot \mathbf{y}_{i_{j^*}})]$, which indicates the right ciphertext.

This already saves the bandwidth since we need the DDH-based anonymous hint system in [LPQ12] to upgrade Libert *et al.*'s concrete ANOBE in order to achieve fast decryption. Even with randomness reuse technique, this will introduce $2 \cdot |S|$ additional group elements to the ciphertext. The perspective here is that $\{[\mathbf{r}^\top \mathbf{A}^\top(\mathbf{x}_{i_j} + \alpha \cdot \mathbf{y}_{i_j})]\}_{j\in[\ell]}$ act as crucial components for achieving IND-CCA security and hints for fast decryption at the same time while they are realized separately in Libert *et al.*'s concrete ANOBE.

Our Second ANOBE: Compressing Ciphertext Again. We now ask:

Can we reduce the ciphertext size if we can tolerate slower decryption?

Observe that we have ℓ group elements (i.e., $\{[\mathbf{r}^\top \mathbf{A}^\top(\mathbf{x}_{i_j} + \alpha \cdot \mathbf{y}_{i_j})]\}_{j\in[\ell]}$) for consistency check (which is necessary for IND-CCA security) in our first ANOBE. If we assume that each recipient can correctly guess which part is intended for him/her, we can see that only one of these ℓ elements will be used in the decryption procedure. Therefore a promising idea is to ask all recipients to share the consistency check process. A direct way to do so is to

$$\text{replace} \quad \{[\mathbf{r}^\top \mathbf{A}^\top(\mathbf{x}_{i_j} + \alpha \cdot \mathbf{y}_{i_j})]\}_{j\in[\ell]} \quad \text{with} \quad [\mathbf{r}^\top \mathbf{A}^\top(\mathbf{x} + \alpha \cdot \mathbf{y})]$$

and publish $[\mathbf{A}^\top \mathbf{x}]$ and $[\mathbf{A}^\top \mathbf{y}]$ in mpk. Unfortunately, there is a fatal issue. To do the consistency check, we should give each user $\mathbf{x}$ and $\mathbf{y}$ directly and they will be leaked to an adversary through any corrupted user. This totally breaks the IND-CCA security. We circumvent the difficulty by making the consistency check public using the technique by Kiltz and Wee [KW15]. In particular, we adapt our first ANOBE to $\mathbb{G}_1$ of a pairing group $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$ and

$$\text{replace} \quad [\mathbf{r}^\top \mathbf{A}^\top(\mathbf{x} + \alpha \cdot \mathbf{y})]_1 \quad \text{with} \quad [\mathbf{r}^\top \mathbf{A}^\top(\mathbf{X} + \alpha \cdot \mathbf{Y})]_1$$

where $\mathbf{X}, \mathbf{Y} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{(k+1)\times(k+1)}$. In the public parameter mpk, we publish

$$([\mathbf{A}^\top \mathbf{X}]_1, [\mathbf{A}^\top \mathbf{Y}]_1) \quad \text{and} \quad ([\mathbf{B}]_2, [\mathbf{XB}]_2, [\mathbf{YB}]_2)$$

where $\mathbf{B} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{(k+1)\times k}$ and the right-hand side part allow *anyone* to *publicly* check the ciphertext consistency.

We have successfully compressed the ciphertext but lose the correctness of decryption since we do not have hint system now. It is easy to fix using *key-binding* symmetric encryption scheme (E, D). That is we pick session key K from the key space of (E, D) and

$$\text{replace} \quad [\mathbf{r}^\top \mathbf{A}^\top \mathbf{k}_{i_j}]_1 \cdot m \quad \text{with} \quad [\mathbf{r}^\top \mathbf{A}^\top \mathbf{k}_{i_j}]_1 \cdot K, \mathsf{E}_K(m).$$

We note that we are not pursuing fast decryption now. We can further get rid of σ by defining α as in Cramer-Shoup PKE [CS98, CS02]. We sketch our second ANOBE as follows:

$$\begin{aligned}
\mathsf{mpk} &: (\mathsf{E}, \mathsf{D}), \mathsf{h};\ \{\ \colorbox{lightgray}{$[\mathbf{A}^\top]_1$}\ , [\mathbf{A}^\top \mathbf{k}_i]_1,\ \colorbox{lightgray}{$[\mathbf{A}^\top \mathbf{X}]_1, [\mathbf{A}^\top \mathbf{Y}]_1$}\ \}_{i \in [n]};\ [\mathbf{B}]_2, [\mathbf{XB}]_2, [\mathbf{YB}]_2 \\
\mathsf{sk}_i &: \mathbf{k}_i \\
\mathsf{ct}_S &: \{\ \colorbox{lightgray}{$[\mathbf{r}^\top \mathbf{A}^\top]_1$}\ , [\mathbf{r}^\top \mathbf{A}^\top \mathbf{k}_{i_j}]_1 \cdot K,\ \colorbox{lightgray}{$\mathsf{E}_K(m)$}\ ,\ \colorbox{lightgray}{$[\mathbf{r}^\top \mathbf{A}^\top (\mathbf{X} + \alpha \cdot \mathbf{Y})]_1$}\ \}_{j \in [\ell]}
\end{aligned}$$

where all terms in gray box are shared by all users/receivers. As our first ANOBE, the reduction loss is constant.

Compared with Libert *et al.*'s concrete ANOBE [LPQ12], our second ANOBE is based on weaker assumptions — we don't require the existence of strongly one-time signature and (E, D) is not necessarily authenticated encryption. Furthermore, in the ciphertext, we share as many components as possible among receivers in the target set, the remaining ℓ group elements seem to be inevitable by the lower bound [KS12].

Organization. Our paper is organized as follows. We review some basic notions in Sect. 2. Our two ANOBE constructions along with security analysis will be presented in Sects. 3 and 4, respectively. We finally conclude the paper in Sect. 5.

2 Preliminaries

Notations. For $n \in \mathbb{N}$, we define $[n] := \{1, 2, \ldots, n\}$. We use $a \leftarrow_{\mathrm{R}} A$ to denote the process of uniformly sampling an element from set A and assigning it to variable a. For two sets S_0, S_1, define $S_0 \triangle S_1 := (S_0 \setminus S_1) \cup (S_1 \setminus S_0)$. "p.p.t." stands for probabilistic polynomial time.

2.1 Anonymous Broadcast Encryption

Algorithms. Let $U := [n]$ be the universe. A *broadcast encryption* (BE) scheme consists of four algorithms $(\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$: Algorithm Setup takes security parameter 1^λ and n as input and outputs a master public key mpk and a master secret key msk; Algorithm KeyGen takes mpk, msk and an index $i \in U$ as input and outputs a secret key sk_i; Algorithm Enc takes mpk, a message m and a subset $S \subseteq U$ as input and outputs a ciphertext ct_S; Algorithm Dec takes mpk, ct_S and sk_i as input and outputs m or a failure symbol $\perp$.

Correctness. For all λ, all $(\mathsf{mpk}, \mathsf{msk}) \leftarrow_{\mathrm{R}} \mathsf{Setup}(1^\lambda, n)$, all m, all $S \subseteq U$, and all $i \in S$, it is required that $\mathsf{Dec}(\mathsf{mpk}, \mathsf{Enc}(\mathsf{mpk}, m, S), \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, i)) = m$.

Chosen-Ciphertext Security and Anonymity. For any adversary $\mathcal{A}$, define

$$\mathsf{Adv}^{\mathsf{BE}}_{\mathcal{A}}(1^\lambda) := \left| \Pr \left[b = b' \;\middle|\; \begin{array}{c} (\mathsf{mpk}, \mathsf{msk}) \leftarrow_{\mathrm{R}} \mathsf{Setup}(1^\lambda, n),\;\; b \leftarrow_{\mathrm{R}} \{0,1\} \\ (m_0, m_1, S_0, S_1) \leftarrow_{\mathrm{R}} \mathcal{A}^{\mathsf{KeyO}(\cdot), \mathsf{DecO}(\cdot,\cdot)}(1^\lambda, \mathsf{mpk}) \\ \mathsf{ct}^* \leftarrow_{\mathrm{R}} \mathsf{Enc}(\mathsf{mpk}, m_b, S_b) \\ b' \leftarrow_{\mathrm{R}} \mathcal{A}^{\mathsf{KeyO}(\cdot), \mathsf{DecO}(\cdot,\cdot)}(1^\lambda, \mathsf{mpk}, \mathsf{ct}^*) \end{array} \right] - \frac{1}{2} \right|$$

where oracles work as follows:

- KeyO: on input i, *key extraction oracle* KeyO outputs $\mathsf{sk}_i \leftarrow_{\mathrm{R}} \mathsf{KeyGen}(\mathsf{msk}, \mathsf{mpk}, i)$ and sets $Q_{\mathsf{sk}} := Q_{\mathsf{sk}} \cup \{i\}$ which is initialized to be $\emptyset$ at the beginning.
- DecO: on input (ct, i), *decryption oracle* DecO outputs $\mathsf{Dec}(\mathsf{mpk}, \mathsf{ct}, \mathsf{sk}_i)$ when ct^* (a.k.a. *challenge ciphertext*) has not been defined or $\mathsf{ct} \neq \mathsf{ct}^*$.

A broadcast encryption scheme achieves chosen-ciphertext security and anonymity (ANO-IND-CCA) if, for all p.p.t. adversary $\mathcal{A}$, $\mathsf{Adv}^{\mathsf{BE}}_{\mathcal{A}}(\lambda)$ is negligible in λ under the restrictions that (1) $|m_0| = |m_1|$ and $|S_0| = |S_1|$; (2) $Q_{\mathsf{sk}} \cap (S_0 \triangle S_1) = \emptyset$; (3) if $Q_{\mathsf{sk}} \cap (S_0 \cap S_1) \neq \emptyset$, then $m_0 = m_1$.

2.2 Prime-Order (Bilinear) Groups

Prime-Order Group. A group generator GGen is a p.p.t. algorithm which takes 1^λ as input and outputs a description $\mathcal{G} := (p, \mathbb{G}, g)$. Here $\mathbb{G}$ is a finite cyclic group of prime order p and g is a random generator of $\mathbb{G}$. Throughout the paper, we will use *implicit representation* [EHK+13]. We let $[a] := g^a \in \mathbb{G}$ for all $a \in \mathbb{Z}_p$. For a matrix $\mathbf{A} = (a_{ij}) \in \mathbb{Z}_p^{m \times n}$, we let $[\mathbf{A}] = (g^{a_{ij}}) \in \mathbb{G}^{m \times n}$.

Prime-Order Bilinear Group. A group generator PGGen is a p.p.t. algorithm which takes 1^λ as input and outputs a description $\mathcal{PG} := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2)$ of (asymmetric) bilinear group. Here $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ are finite cyclic groups of prime order p and e is an admissible bilinear map. $g_1 \in \mathbb{G}_1$ and $g_2 \in \mathbb{G}_2$ are random generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, and $g_T := e(g_1, g_2)$ will be a generator of group $\mathbb{G}_T$. The implicit representation is also be applied to prime-order *bilinear* groups: We let $[a]_s := g_s^a \in \mathbb{G}_s$ for all $a \in \mathbb{Z}_p$ and $s \in \{1, 2, T\}$. The notation can be easily extended to matrices analogously and we let $e([\mathbf{A}]_1, [\mathbf{B}]_2) := [\mathbf{AB}]_T$ for matrices $\mathbf{A}$ and $\mathbf{B}$ when the multiplication is well-defined.

Cryptographic Assumption. 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 may assume that for all $\mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{D}_k$, the first k rows of $\mathbf{A}$ form an invertible matrix.

We will use the $\mathcal{D}_k$-Matrix Diffie-Hellman ($\mathcal{D}_k$-MDDH) assumption in $\mathbb{G}$ described as follows. The $\mathcal{D}_k$-MDDH assumption in $\mathbb{G}_1$ and $\mathbb{G}_2$ are analogous.

Assumption 1 ($\mathcal{D}_k$-MDDH). *We say that the $\mathcal{D}_k$-Matrix Diffie-Hellman assumption holds relative to* GGen*, if for any p.p.t. adversary $\mathcal{A}$, the following advantage function is negligible in λ.*

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

where $\mathcal{G} \leftarrow_{\mathrm{R}} \mathsf{GGen}(1^\lambda)$, $\mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{D}_k$, $\mathbf{s} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$, *and* $\mathbf{u} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}$.

The famous k-Linear (k-Lin) assumption is an instantiation of the $\mathcal{D}_k$-MDDH assumption. The classical *decisional Diffie-Hellman* (DDH) assumption (a.k.a *symmetric external Diffie-Hellman* (SXDH) assumption in *asymmetric* bilinear groups) is just the k-Lin assumption with $k = 1$. See [EHK+13] for more details.

For bilinear groups, we also use the $\mathcal{D}_k$-Matrix Kernel Diffie-Hellman ($\mathcal{D}_k$-KerMDH) Assumption [MRV16], which is implied by the $\mathcal{D}_k$-MDDH assumption.

Assumption 2 ($\mathcal{D}_k$-KerMDH). *Let $s \in \{1,2\}$. We say that the $\mathcal{D}_k$-Kernel Matrix Diffie-Hellman Assumption holds relative to* PGGen*, if for any p.p.t. adversary $\mathcal{A}$, the following advantage function is negligible in λ.*

$$\mathsf{Adv}^{\mathsf{kmdh}}_{\mathcal{A},\mathbb{G}_s}(\lambda) := \Pr[\mathbf{A}^\top\mathbf{a}^\perp = \mathbf{0} \wedge \mathbf{a}^\perp \neq \mathbf{0} \mid [\mathbf{a}^\perp]_{3-s} \leftarrow_{\mathrm{R}} \mathcal{A}(\mathcal{PG},[\mathbf{A}]_s)]$$

where $\mathcal{PG} \leftarrow_{\mathrm{R}} \mathsf{PGGen}(1^\lambda), \mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{D}_k$.

2.3 Cryptographic Primitives

Our constructions will use the following cryptographic primitives:

- A semantically secure and key-binding symmetric encryption scheme (E,D) with key space $\mathcal{K}$. Let $\mathsf{E}_K(\cdot)$ and $\mathsf{D}_K(\cdot)$ denote the encryption and decryption procedures under secret key $K \in \mathcal{K}$. By *key-binding* [Fis99], we mean that, for any message m and any secret key $K \in \mathcal{K}$, there exists no $K' \in \mathcal{K}$ such that $K \neq K'$ and $\mathsf{D}_{K'}(\mathsf{E}_K(m)) \neq \perp$ (Here $\perp$ indicates a decryption failure).
- A family of collision-resistant hash function $\mathcal{H}$. It ensures that, given $\mathsf{h} \leftarrow_{\mathrm{R}} \mathcal{H}$, it is hard to find $x \neq y$ such that $\mathsf{h}(x) = \mathsf{h}(y)$ (i.e., a collision).
- A strongly unforgeable one-time signature scheme $(\mathsf{Gen}_{\mathsf{ots}},\mathsf{Sign},\mathsf{Ver})$. Let $(\mathsf{pk}_{\mathsf{ots}},\mathsf{sk}_{\mathsf{ots}}) \leftarrow_{\mathrm{R}} \mathsf{Gen}_{\mathsf{ots}}(1^\lambda)$ be a verification key and a signing key. It is guaranteed that, given $\mathsf{pk}_{\mathsf{ots}}$ and a signature $\sigma \leftarrow_{\mathrm{R}} \mathsf{Sign}(\mathsf{sk}_{\mathsf{ots}},m)$ for some adversarially chosen message m, it is infeasible to output another message-signature pair $(m^*,\sigma^*) \neq (m,\sigma)$ satisfying $\mathsf{Ver}(\mathsf{pk}_{\mathsf{ots}},m^*,\sigma^*)=1$.

We will use $\mathsf{Adv}^{\mathsf{se}}_{\mathcal{A}}(\lambda)$, $\mathsf{Adv}^{\mathsf{hash}}_{\mathcal{A}}(\lambda)$ and $\mathsf{Adv}^{\mathsf{ots}}_{\mathcal{A}}(\lambda)$ to denote the advantage of adversary $\mathcal{A}$ in violating the security of above primitives under security parameter λ. Formal definitions can be found in the full version of the paper.

2.4 Core Lemma

We review the core lemma in [KW15].

Lemma 1 (Core lemma, [KW15]). *Let $k \in \mathbb{N}$. For any $\mathbf{A}, \mathbf{B} \in \mathbb{Z}_p^{(k+1)\times k}$ and any (possibly unbounded) adversary $\mathcal{A}$, we have*

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

where $\mathcal{O}(\alpha^*) \to \mathbf{X} + \alpha^* \cdot \mathbf{Y}$ may only be called one time.

3 Tightly Secure ANOBE with Fast Decryption

3.1 Construction

Our first broadcast encryption scheme is described as follows.

- $\mathsf{Setup}(1^\lambda, n)$: Run $\mathcal{G} := (p, \mathbb{G}, g) \leftarrow_{\mathrm{R}} \mathsf{GGen}(1^\lambda)$. Sample

$$\mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{D}_k \quad \text{and} \quad \mathbf{k}_i, \mathbf{x}_i, \mathbf{y}_i \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1} \quad \text{for} \quad i \in [n].$$

  Select a strongly unforgeable one-time signature scheme $(\mathsf{Gen}_{\mathsf{ots}}, \mathsf{Sig}, \mathsf{Ver})$ and a hash function $\mathsf{h} : \{0,1\}^* \to \mathbb{Z}_p$ from $\mathcal{H}$. The master public key is

$$\mathsf{mpk} := (\mathcal{G}, \mathsf{h}, (\mathsf{Gen}_{\mathsf{ots}}, \mathsf{Sig}, \mathsf{Ver}), [\mathbf{A}], \{[\mathbf{A}^\top\mathbf{k}_i], [\mathbf{A}^\top\mathbf{x}_i], [\mathbf{A}^\top\mathbf{y}_i]\}_{i=1}^n)$$

  and the master secret key is $\mathsf{msk} := (\{\mathbf{k}_i, \mathbf{x}_i, \mathbf{y}_i\}_{i=1}^n)$.
- $\mathsf{KeyGen}(\mathsf{msk}, \mathsf{mpk}, i)$: Output the secret key $\mathsf{sk}_i = (\mathbf{k}_i, \mathbf{x}_i, \mathbf{y}_i)$.
- $\mathsf{Enc}(\mathsf{mpk}, m, S)$: Let $\ell := |S|$ and $S = \{i_1, \ldots, i_\ell\} \subseteq U = [n]$. Sample $\mathbf{r} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$ and compute $[\mathbf{u}^\top] := [\mathbf{r}^\top\mathbf{A}^\top]$. Generate $(\mathsf{sk}_{\mathsf{ots}}, \mathsf{pk}_{\mathsf{ots}}) \leftarrow_{\mathrm{R}} \mathsf{Gen}_{\mathsf{ots}}(1^\lambda)$, compute $\alpha := \mathsf{h}(\mathsf{pk}_{\mathsf{ots}})$ and $c_1 := [\mathbf{r}^\top\mathbf{A}^\top\mathbf{k}_{i_1}] \cdot m, v_1 := [\mathbf{r}^\top\mathbf{A}^\top(\mathbf{x}_{i_1} + \alpha \cdot \mathbf{y}_{i_1})], \ldots, c_\ell := [\mathbf{r}^\top\mathbf{A}^\top\mathbf{k}_{i_\ell}] \cdot m, v_\ell := [\mathbf{r}^\top\mathbf{A}^\top(\mathbf{x}_{i_\ell} + \alpha \cdot \mathbf{y}_{i_\ell})]$. Choose a random permutation τ over $[\ell]$ and compute $\sigma := \mathsf{Sig}(\mathsf{sk}_{\mathsf{ots}}, ([\mathbf{u}^\top], c_{\tau(1)}, v_{\tau(1)}, \ldots, c_{\tau(\ell)}, v_{\tau(\ell)}))$. The ciphertext is

$$\mathsf{ct} := ([\mathbf{u}^\top], c_{\tau(1)}, v_{\tau(1)}, \ldots, c_{\tau(\ell)}, v_{\tau(\ell)}, \mathsf{pk}_{\mathsf{ots}}, \sigma).$$

- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{ct}, \mathsf{sk}_i)$: Parse the ciphertext ct as $([\mathbf{u}^\top], \bar{c}_1, \bar{v}_1, \ldots, \bar{c}_\ell, \bar{v}_\ell, \mathsf{pk}_{\mathsf{ots}}, \sigma)$ and the secret key sk_i as $(\mathbf{k}_i, \mathbf{x}_i, \mathbf{y}_i)$. Return $\perp$ if

$$\mathsf{Ver}(\mathsf{pk}_{\mathsf{ots}}, ([\mathbf{u}^\top], \bar{c}_1, \bar{v}_1, \ldots, \bar{c}_\ell, \bar{v}_\ell), \sigma) = 0,$$

  otherwise, compute

$$v := [\mathbf{u}^\top(\mathbf{x}_i + \alpha \cdot \mathbf{y}_i)],$$

  where $\alpha = \mathsf{h}(\mathsf{pk}_{\mathsf{ots}})$. If there exists $j \in [\ell]$ such that $v = \bar{v}_j$, return $m' := \bar{c}_j/[\mathbf{u}^\top\mathbf{k}_i]$; otherwise, return $\perp$.

It is direct to check the correctness.

3.2 Security Result and Proof Overview

We prove the following theorem.

Theorem 1. *Our broadcast encryption scheme in Sect. 3.1 is adaptively ANO-IND-CCA secure assuming that: (1) $\mathcal{H}$ is collision-resistant; (2) the $\mathcal{D}_k$-MDDH assumption holds in $\mathbb{G}$; (3) signature scheme $(\mathsf{Gen_{ots}}, \mathsf{Sig}, \mathsf{Ver})$ is strongly unforgeable under one-time chosen message attack. Concretely, for any adversary $\mathcal{A}$, there exist algorithms $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$ such that*

$$\mathsf{Adv}^{\mathsf{BE}}_{\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{mddh}}_{\mathbb{G},\mathcal{B}_1}(\lambda) + \mathsf{Adv}^{\mathsf{ots}}_{\mathcal{B}_2}(\lambda) + \mathsf{Adv}^{\mathsf{hash}}_{\mathcal{B}_3}(\lambda) + O(1/p)$$

and $\mathsf{Time}(\mathcal{B}_1), \mathsf{Time}(\mathcal{B}_2), \mathsf{Time}(\mathcal{B}_3) \approx \mathsf{Time}(\mathcal{A})$.

We prove the theorem via the following game sequence. A proof sketch for each step will be given and more details can be found in the full paper.

Game_0**.** This game is identical to the real game described in Sect. 2.1. The challenge ciphertext for (m_0, m_1, S_0, S_1) where $S_0 = \{i_{1,0}, \ldots, i_{\ell,0}\}$ and $S_1 = \{i_{1,1}, \ldots, i_{\ell,1}\}$ is of form

$$\mathsf{ct}^* := (\,\mathsf{ct}_1^* := ([\mathbf{u}^{*\top}], c_1^*, v_1^*, \ldots, c_\ell^*, v_\ell^*),\ \mathsf{pk}^*_{\mathsf{ots}},\ \sigma^* := \mathsf{Sig}(\mathsf{sk}^*_{\mathsf{ots}}, \mathsf{ct}_1^*)\,)$$

where $\mathbf{u}^* \leftarrow_{\mathrm{R}} \mathsf{span}(\mathbf{A})$, $(\mathsf{sk}^*_{\mathsf{ots}}, \mathsf{pk}^*_{\mathsf{ots}}) \leftarrow_{\mathrm{R}} \mathsf{Gen_{ots}}(1^\lambda)$, and we compute

$$c_j^* = [\mathbf{u}^{*\top}\mathbf{k}_{i_{\tau(j),b}}] \cdot m_b \quad \text{and} \quad v_j^* = [\mathbf{u}^{*\top}(\mathbf{x}_{i_{\tau(j),b}} + \alpha^* \cdot \mathbf{y}_{i_{\tau(j),b}})], \quad \forall j \in [\ell]$$

with $b \leftarrow_{\mathrm{R}} \{0,1\}$, $\alpha^* = \mathsf{h}(\mathsf{pk}^*_{\mathsf{ots}})$ and a random permutation τ over $[\ell]$. On input (ct, i), DecO parses

$$\mathsf{ct} = (\mathsf{ct}_1 = ([\mathbf{u}^\top], c_1, v_1, \ldots, c_\ell, v_\ell), \mathsf{pk_{ots}}, \sigma),$$

and rejects the query if

$$(a)\quad \mathsf{ct} = \mathsf{ct}^* \quad \text{or} \quad (b)\quad \mathsf{Ver}(\mathsf{pk_{ots}}, \mathsf{ct}_1, \sigma) = 0.$$

Then compute $v = [\mathbf{u}^\top(\mathbf{x}_i + \alpha \cdot \mathbf{y}_i)]$ with $\alpha = \mathsf{h}(\mathsf{pk_{ots}})$. If there exists $j \in [\ell]$ such that $v = v_j$, return $m' := c_j/[\mathbf{u}^\top\mathbf{k}_i]$; otherwise, return $\perp$. Let Win_i denote the event that $\mathcal{A}$ in Game_i guesses b correctly. Since Game_0 perfectly simulates the real game, we have $\mathsf{Adv}^{\mathsf{BE}}_{\mathcal{A}}(1^\lambda) = |\Pr[\mathsf{Win}_0] - 1/2|$.

Game_1**.** This game is identical to Game_0 except that we sample $\mathbf{u}^* \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}$ when generating the challenge ciphertext ct^*. It is easy to see that this game is indistinguishable from Game_0 under the $\mathcal{D}_k$-MDDH assumption. Formally, we have the following lemma.

Lemma 2 ($\mathsf{Game}_1 \approx_c \mathsf{Game}_0$)**.** *There exists an adversary $\mathcal{B}_1$ such that*

$$|\Pr[\mathsf{Win}_1] - \Pr[\mathsf{Win}_0]| \leq \mathsf{Adv}^{\mathsf{mddh}}_{\mathbb{G},\mathcal{B}_1}(\lambda).$$

Game_2. This game is identical to Game_1 except that DecO, on input (ct, i), rejects the query if (a) or (b) or

$$(c) \quad \mathsf{pk}_{\mathsf{ots}} = \mathsf{pk}^*_{\mathsf{ots}}.$$

This game is identical to Game_1 until $\mathcal{A}$ submits a query with $\mathsf{pk}_{\mathsf{ots}} = \mathsf{pk}^*_{\mathsf{ots}}$ which survives under condition (a) and (b). However σ in such a query will violate the strong unforgeability of $(\mathsf{Gen}_{\mathsf{ots}}, \mathsf{Sig}, \mathsf{Ver})$, and this game is indistinguishable from Game_1. Formally, we have the following lemma.

Lemma 3 **($\mathsf{Game}_2 \approx_c \mathsf{Game}_1$).** *There exists an adversary $\mathcal{B}_2$ such that*

$$|\Pr[\mathsf{Win}_2] - \Pr[\mathsf{Win}_1]| \leq \mathsf{Adv}^{\mathsf{ots}}_{\mathcal{B}_2}(\lambda).$$

Game_3. This game is identical to Game_2 except the following substitution:

$$(c) \quad \mathsf{pk}_{\mathsf{ots}} = \mathsf{pk}^*_{\mathsf{ots}} \quad \longmapsto \quad (c') \quad \alpha = \alpha^*$$

This game is identical to Game_2 until $\mathcal{A}$ submits a query with $\mathsf{pk}_{\mathsf{ots}} \neq \mathsf{pk}^*_{\mathsf{ots}}$ but $\alpha = \alpha^*$. This immediately violates the collision-resistance of $\mathcal{H}$, and this game is indistinguishable from Game_2. Formally, we have the following lemma.

Lemma 4 **($\mathsf{Game}_3 \approx_c \mathsf{Game}_2$).** *There exists an algorithm $\mathcal{B}_3$ such that*

$$|\Pr[\mathsf{Win}_3] - \Pr[\mathsf{Win}_2]| \leq \mathsf{Adv}^{\mathsf{hash}}_{\mathcal{B}_3}(\lambda).$$

Game_4. This game is identical to Game_3 except that except that DecO, on input (ct, i), rejects the query if (a) or (b) or (c') or

$$(d) \quad \mathbf{u} \notin \mathsf{span}(\mathbf{A})$$

We have the following lemma stating that this game is statistically indistinguishable with Game_3.

Lemma 5 **($\mathsf{Game}_4 \approx_s \mathsf{Game}_3$).** $|\mathsf{Win}_4 - \mathsf{Win}_3| \leq O(1/p)$.
Let q_D be the number of decryption queries. The lemma can be proved in q_D steps. In the j-th step, assuming that the first $j-1$ decryption queries have been processed with condition (d), we demonstrate that the j-th query will finally be rejected if it survives under condition $(a), (b), (c')$ with $\mathbf{u} \notin \mathsf{span}(\mathbf{A})$. In other words, we can introduce condition (d) here without changing adversary's view. The proof (for the j-th step) relies on the observation that we leak no more information than $\{\mathbf{A}^\top \mathbf{x}_\eta, \mathbf{A}^\top \mathbf{y}_\eta\}_{\eta \in [n]}$ when answering the first $j-1$ queries to DecO. With the help of condition (c'), which ensures that $\alpha \neq \alpha^*$, we can claim that $\mathbf{u}^\top(\mathbf{x}_i + \alpha \cdot \mathbf{y}_i)$ is independently and uniformly distributed and thus hard to guess.

Finally, we have the following lemma which proves Theorem 1 when combining with all previous lemmas and claims.

Lemma 6. $\Pr[\mathsf{Win}_4] = 1/2$.

This follows from the fact that $(\mathbf{u}^*\mathbf{k}_i, \mathbf{u}^*(\mathbf{x}_i + \alpha \cdot \mathbf{y}_i))$ are uniformly distributed over $\mathbb{G}^2$, especially unrelated to b, for all $i \in S_b$ (resp. $i \in S_b/S_{1-b}$) when $Q_{\mathsf{sk}} \cap (S_0 \cap S_1) = \emptyset$ (resp. $Q_{\mathsf{sk}} \cap (S_0 \cap S_1) \neq \emptyset$), conditioned on $\mathsf{mpk}, \mathsf{KeyO}$ and DecO. The analysis is similar to that for Lemma 5.

Perspective. Lemmas 5 and 6 are at the core of our proof. Although our proofs still rely on the proof technique of underlying Cramer-Shoup PKE, we get rid of large reduction loss by carrying out the argument in the broadcast setting *directly*. In particular, we employ the technique beneath the core lemma from Kiltz and Wee [KW15] (see Lemma 1), which allows us to take *all* users into account in a *non-adaptive* way first and then upgrade to the adaptive setting for free. This avoids guessing adversary's behaviour in the simulation which caused large security loss in Libert *et al.*'s work [LPQ12]. Furthermore, we note that our proof indeed involves *robustness* [ABN10, Moh10, LPQ12] but in an *implicit* manner since we are not working with generic PKE anymore.

4 Tightly Secure ANOBE with Shorter Ciphertext

4.1 Construction

- $\mathsf{Setup}\ (1^\lambda, n)$: Run $\mathcal{PG} := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2) \leftarrow_{\mathrm{R}} \mathsf{PGGen}(1^\lambda)$. Sample
$$\mathbf{A}, \mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k,\ \mathbf{X}, \mathbf{Y} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{(k+1)\times(k+1)},\ \mathbf{k}_i \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1} \quad \text{for } i \in [n].$$
Select a key-binding secure symmetric encryption scheme (E, D) with the key space $\mathcal{K} := \mathbb{G}_1$ and a collision-resilient hash function $\mathsf{h} \leftarrow_{\mathrm{R}} \mathcal{H}$ mapping from $\{0,1\}^*$ to $\mathbb{Z}_p$. The master public key is
$$\mathsf{mpk} := \left(\mathcal{PG}, (\mathsf{E}, \mathsf{D}), \mathsf{h};\ \begin{array}{ll} [\mathbf{A}^\top]_1,\ \{[\mathbf{A}^\top \mathbf{k}_i]_1\}_{i=1}^n, & [\mathbf{A}^\top \mathbf{X}]_1,\ [\mathbf{A}^\top \mathbf{Y}]_1 \\ [\mathbf{B}]_2, & [\mathbf{XB}]_2,\ \ [\mathbf{YB}]_2 \end{array} \right)$$
and the master secret key is $\mathsf{msk} := \{\mathbf{k}_i\}_{i=1}^n$.
- $\mathsf{KeyGen}\ (\mathsf{msk}, \mathsf{mpk}, i)$: Output the secret key $\mathsf{sk}_i := \mathbf{k}_i$.
- $\mathsf{Enc}\ (\mathsf{mpk}, m, S)$: Let $\ell := |S|$ and $S = \{i_1, \ldots, i_\ell\} \subseteq U$. Sample $\mathbf{r} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$ and compute $[\mathbf{u}^\top]_1 := [\mathbf{r}^\top \mathbf{A}^\top]_1$. Select session key $K \leftarrow_{\mathrm{R}} \mathbb{G}_1$ and compute
$$c_0 := \mathsf{E}_K(m),\ c_1 := [\mathbf{r}^\top \mathbf{A}^\top \mathbf{k}_{i_1}]_1 \cdot K,\ \ldots,\ c_\ell := [\mathbf{r}^\top \mathbf{A}^\top \mathbf{k}_{i_\ell}]_1 \cdot K$$
Choose a random permutation τ over $[\ell]$ and compute
$$[\boldsymbol{\pi}]_1 := [\mathbf{r}^\top \mathbf{A}^\top (\mathbf{X} + \alpha \cdot \mathbf{Y})]_1$$
where $\alpha := \mathsf{h}([\mathbf{u}^\top]_1, c_0, c_{\tau(1)}, \ldots, c_{\tau(\ell)})$. The ciphertext is
$$\mathsf{ct} := (\ [\mathbf{u}^\top]_1,\ c_0,\ c_{\tau(1)},\ \ldots,\ c_{\tau(\ell)},,\ [\boldsymbol{\pi}]_1\ ).$$
- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{ct}, \mathsf{sk}_i)$: Parse ct as $([\mathbf{u}^\top]_1, c_0, \bar{c}_1, \ldots, \bar{c}_\ell, [\boldsymbol{\pi}]_1)$ and sk_i as $\mathbf{k}_i$. Compute $\alpha = \mathsf{h}([\mathbf{u}^\top]_1, c_0, \bar{c}_1, \ldots, \bar{c}_\ell)$ and check
$$e([\boldsymbol{\pi}]_1, [\mathbf{B}]_2) \overset{?}{=} e([\mathbf{u}^\top]_1, [(\mathbf{X} + \alpha \cdot \mathbf{Y})\mathbf{B}]_2). \tag{1}$$
If Eq. (1) does not hold, return $\perp$; otherwise, do the following two steps from $j := 1$.
  1. Compute $K' := \bar{c}_j / [\mathbf{u}^\top \mathbf{k}_i]_1$ and $m' := \mathsf{D}_{K'}(c_0)$. If $m' \neq \perp$, return m' and halt; otherwise, go to the second step.
  2. If $j = \ell$, return $\perp$ and halt; otherwise, do the first step with $j := j + 1$.

Correctness. For any ciphertext $\mathsf{ct} := ([\mathbf{u}^\top]_1, c_0, \bar{c}_1, \ldots, \bar{c}_\ell, [\boldsymbol{\pi}]_1)$ for set $S \subseteq U$ produced by Enc, we have

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

where $\alpha = \mathsf{h}([\mathbf{u}^\top]_1, c_0, \bar{c}_1, \ldots, \bar{c}_\ell)$. That is the ciphertext always satisfies Eq. (1). Given a secret key $\mathsf{sk}_i = \mathbf{k}_i$ for $i \in S$, we know that there exists $i' \in [\ell]$ such that $c_{i'} = [\mathbf{r}^\top \mathbf{A}^\top \mathbf{k}_i]_1 \cdot K$. The correctness of our ANOBE then follows from the following two observations:

1. For each $j < i'$, we know that $c_j = [\mathbf{r}^\top \mathbf{A}^\top \mathbf{k}_{j'}]_1 \cdot K$ for some $j' \in S \setminus \{i\}$, and thus we have
$$c_j / [\mathbf{u}^\top \mathbf{k}_i]_1 \neq K$$
with overwhelming probability. From the key-binding feature of (E, D), the decryption algorithm Dec will return nothing before the i'-th iteration.
2. It is easy to see that
$$c_{i'} / [\mathbf{u}^\top \mathbf{k}_i]_1 = K.$$
By the correctness of (E, D), the decryption algorithm Dec will return m in the i'-th iteration.

4.2 Security Result and Proof Overview

We prove the following theorem.

Theorem 2. *Our broadcast encryption described in Sect. 4.1 is 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) (E, D) is semantically secure. Concretely, for any adversary $\mathcal{A}$, there exist algorithms $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3, \mathcal{B}_4$, such that*

$$\mathsf{Adv}^{\mathsf{BE}}_{\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{B}_1, \mathbb{G}_1}(\lambda) + \mathsf{Adv}^{\mathsf{hash}}_{\mathcal{B}_2}(\lambda) + \mathsf{Adv}^{\mathsf{kmdh}}_{\mathcal{B}_3, \mathbb{G}_2}(\lambda) + 2 \cdot \mathsf{Adv}^{\mathsf{se}}_{\mathcal{B}_4}(\lambda) + O(1/p)$$

and $\mathsf{Time}(\mathcal{B}_1), \mathsf{Time}(\mathcal{B}_2), \mathsf{Time}(\mathcal{B}_3), \mathsf{Time}(\mathcal{B}_4) \approx \mathsf{Time}(\mathcal{A})$.

We prove the theorem via the following game sequence. A proof sketch for each step will be given and more details can be found in the full paper.

Game_0**.** This game is identical to the real game described in Sect. 2.1. The challenge ciphertext for (m_0, m_1, S_0, S_1) where $S_0 = \{i_{1,0}, \ldots, i_{\ell,0}\}$ and $S_1 = \{i_{1,1}, \ldots, i_{\ell,1}\}$ is of form

$$\mathsf{ct}^* := (\ \mathsf{ct}_1^* := ([\mathbf{u}^{*\top}]_1, c_0^*, c_1^*, \ldots, c_\ell^*),\ [\boldsymbol{\pi}^*]_1 := [\mathbf{u}^{*\top}(\mathbf{X} + \alpha^* \cdot \mathbf{Y})]_1\ )$$

where $\mathbf{u}^* \leftarrow_{\mathrm{R}} \mathsf{span}(\mathbf{A})$, $\alpha^* = \mathsf{h}(\mathsf{ct}_1^*)$ and we compute

$$c_0^* = \mathsf{E}_{K^*}(m_b) \quad \text{and} \quad c_j^* = [\mathbf{u}^{*\top} \mathbf{k}_{i_{\tau(j),b}}]_1 \cdot K^*, \quad \forall j \in [\ell]$$

with $K^* \leftarrow_{\mathrm{R}} \mathbb{G}_1$ and random permutation τ over $[\ell]$. On input (ct, i), parse

$$\mathsf{ct} = (\mathsf{ct}_1 = ([\mathbf{u}^\top]_1, c_0, c_1, \ldots, c_\ell), [\boldsymbol{\pi}]_1),$$

compute $\alpha = \mathsf{h}(\mathsf{ct}_1)$ and reject the query if

$$(a) \quad \mathsf{ct} = \mathsf{ct}^* \quad \text{or} \quad (b) \quad e([\boldsymbol{\pi}]_1, [\mathbf{B}]_2) \neq e([\mathbf{u}^\top]_1, [(\mathbf{X} + \alpha \cdot \mathbf{Y})\mathbf{B}]_2).$$

Then recover m using $\mathbf{k}_i$ as Dec and return m. We let Win_i denote the event that $\mathcal{A}$ guesses b correctly in Game_i. Since Game_0 perfectly simulates the real game, we have $\mathsf{Adv}^{\mathsf{BE}}_{\mathcal{A}}(1^\lambda) = |\Pr[\mathsf{Win}_0] - 1/2|$.

Game_1. This game is identical to Game_0 except that we sample $\mathbf{u}^* \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}$ when generating the challenge ciphertext ct^*. This game is indistinguishable from Game_0 under the $\mathcal{D}_k$-MDDH assumption. Formally, we have the following lemma and the proof is analgous to that for Lemma 2.

Lemma 7 ($\mathsf{Game}_1 \approx_c \mathsf{Game}_0$). *There exists an adversary* $\mathcal{B}_1$ such that

$$|\Pr[\mathsf{Win}_1] - \Pr[\mathsf{Win}_0]| \leq \mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{B}_1, \mathbb{G}_1}(\lambda)$$

Game_2. This game is identical to Game_1 except that DecO, on input (ct, i), returns $\perp$ if (a) or (b) or

$$(c) \quad \mathsf{ct}_1 \neq \mathsf{ct}_1^* \text{ but } \alpha = \alpha^*.$$

By the collision-resilience of $\mathcal{H}$, this game is indistinguishable from Game_1. Formally, we have the following lemma and the proof is similar to that for Lemma 4.

Lemma 8 ($\mathsf{Game}_2 \approx_c \mathsf{Game}_1$). *There exists an algorithm* $\mathcal{B}_2$ *such that*

$$|\Pr[\mathsf{Win}_2] - \Pr[\mathsf{Win}_1]| \leq \mathsf{Adv}^{\mathsf{hash}}_{\mathcal{B}_2}(\lambda)$$

Game_3. This game is identical to Game_2 except the following substitution:

$$(b)\, e([\boldsymbol{\pi}]_1, [\mathbf{B}]_2) \neq e([\mathbf{u}^\top]_1, [(\mathbf{X} + \alpha \cdot \mathbf{Y})\mathbf{B}]_2) \longmapsto (b')\, [\boldsymbol{\pi}]_1 \neq [\mathbf{u}^\top(\mathbf{X} + \alpha \cdot \mathbf{Y})]_1.$$

This game is the same as Game_2 until $\mathcal{A}$ sends DecO a query which is rejected by condition (b') but survives under condition (b). One can see that such a query immediately gives a solution to the $\mathcal{D}_k$-KerMDH problem w.r.t $[\mathbf{B}]_2$. Formally, we have the following lemma.

Lemma 9 ($\mathsf{Game}_3 \approx_c \mathsf{Game}_2$). *There exists an algorithm* $\mathcal{B}_3$ *such that*

$$|\Pr[\mathsf{Win}_3] - \Pr[\mathsf{Win}_2]| \leq \mathsf{Adv}^{\mathsf{kmdh}}_{\mathcal{B}_3, \mathbb{G}_2}(\lambda)$$

Game_4. This game is identical to Game_3 except the following substitution

$$(b')\, [\boldsymbol{\pi}]_1 \neq [\mathbf{u}^\top(\mathbf{X} + \alpha \cdot \mathbf{Y})]_1 \longmapsto (b'')\, \mathbf{u} \notin \mathsf{span}(\mathbf{A}) \parallel [\boldsymbol{\pi}]_1 \neq [\mathbf{u}^\top(\mathbf{X} + \alpha \cdot \mathbf{Y})]_1.$$

Here "$\|$" denotes the OR operation which neglects the second operand if the first one is satisfied. We have the following lemma stating that this game is statistically close to Game_3.

Lemma 10 ($\mathsf{Game}_4 \approx_s \mathsf{Game}_3$). $|\Pr[\mathsf{Win}_4] - \Pr[\mathsf{Win}_3]| \leq O(1/p)$.
Let q_D be the number of decryption queries. The lemma will be proved in q_D steps. In the j-th step, assuming that the first $j-1$ decryption queries have been processed with condition (b''), we demonstrate that the j-th query with $\mathbf{u} \notin \mathsf{span}(\mathbf{A})$ can be rejected by condition $(a), (b'), (c)$ with high probability. This simply follows from Lemma 1 (the core lemma).

To complete the proof of Theorem 2, we show the following lemma.

Lemma 11. (Bounding $\Pr[\mathsf{Win}_4]$**).** *There exists an algorithm* $\mathcal{B}_4$ *such that*

$$\Pr[\mathsf{Win}_4] \leq 1/2 + 2 \cdot \mathsf{Adv}^{\mathsf{se}}_{\mathcal{B}_4}(\lambda)$$

To prove the lemma, we consider two cases: (1) when $Q_{\mathsf{sk}} \cap (S_0 \cap S_1) = \emptyset$, we can prove that $[\mathbf{u}^{*\top}\mathbf{k}_i]_1$ for $i \in S_b$ are independently and uniformly distributed over $\mathbb{G}_1$, which hide both S_b and K^*. The proof is similar to the proof of Lemma 6. Then the semantic security of (E, D) allows us to hide m_b; (2) when $Q_{\mathsf{sk}} \cap (S_0 \cap S_1) \neq \emptyset$, we can only prove that $[\mathbf{u}^{*\top}\mathbf{k}_i]_1$ for $i \in S_b \backslash S_{1-b}$ are randomly distributed, but it is sufficient for proving the lemma since $m_0 = m_1$.

5 Conclusion

In this paper, we described two concrete ANOBE schemes. The first one is an instantiation of Libert *et al.*'s generic ANOBE. However, by working out the proof directly, we achieved a constantly tight reduction to standard assumptions. Furthermore, we pointed out that this scheme supports fast decryption for free and thus enjoys shorter ciphertexts. By the second scheme, we showed how to shorten the ciphertext again while preserving the tightness at the cost of slower decryption.

Acknowledgment. We greatly thank Benoît Libert for his encouragement and support. We also thank all anonymous reviewers for their constructive comments.

References

[ABN10] Abdalla, M., Bellare, M., Neven, G.: Robust encryption. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 480–497. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-11799-2_28

[BBS03] Bellare, M., Boldyreva, A., Staddon, J.: Randomness re-use in multi-recipient encryption schemeas. In: Desmedt, Y.G. (ed.) PKC 2003. LNCS, vol. 2567, pp. 85–99. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-36288-6_7

[BBW06] Barth, A., Boneh, D., Waters, B.: Privacy in encrypted content distribution using private broadcast encryption. In: Di Crescenzo, G., Rubin, A. (eds.) FC 2006. LNCS, vol. 4107, pp. 52–64. Springer, Heidelberg (2006). https://doi.org/10.1007/11889663_4

[Ber91] Berkovits, S.: How to broadcast a secret. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 535–541. Springer, Heidelberg (1991). https://doi.org/10.1007/3-540-46416-6_50

[BGW05] Boneh, D., Gentry, C., Waters, B.: Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 258–275. Springer, Heidelberg (2005). https://doi.org/10.1007/11535218_16

[BSW11] Boneh, D., Sahai, A., Waters, B.: Functional encryption: definitions and challenges. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 253–273. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19571-6_16

[CCS09] Camenisch, J., Chandran, N., Shoup, V.: A public key encryption scheme secure against key dependent chosen plaintext and adaptive chosen ciphertext attacks. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 351–368. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-01001-9_20

[CGW15] Chen, J., Gay, R., Wee, H.: Improved dual system ABE in prime-order groups via predicate encodings. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9057, pp. 595–624. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46803-6_20

[CHK04] Canetti, R., Halevi, S., Katz, J.: Chosen-ciphertext security from identity-based encryption. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 207–222. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24676-3_13

[CS98] Cramer, R., Shoup, V.: A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 13–25. Springer, Heidelberg (1998). https://doi.org/10.1007/BFb0055717

[CS02] Cramer, R., Shoup, V.: Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 45–64. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-46035-7_4

[DPP07] Delerablée, C., Paillier, P., Pointcheval, D.: Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys. In: Takagi, T., Okamoto, T., Okamoto, E., Okamoto, T. (eds.) Pairing 2007. LNCS, vol. 4575, pp. 39–59. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-73489-5_4

[EHK+13] Escala, A., Herold, G., Kiltz, E., Ràfols, C., Villar, J.: An algebraic framework for Diffie-Hellman assumptions. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8043, pp. 129–147. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40084-1_8

[Fis99] Fischlin, M.: Pseudorandom function tribe ensembles based on one-way permutations: improvements and applications. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 432–445. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48910-X_30

[FN94] Fiat, A., Naor, M.: Broadcast encryption. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 480–491. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-48329-2_40

[FP12] Fazio, N., Perera, I.M.: Outsider-anonymous broadcast encryption with sublinear ciphertexts. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 225–242. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-30057-8_14

[GHKW16] Gay, R., Hofheinz, D., Kiltz, E., Wee, H.: Tightly CCA-secure encryption without pairings. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016. LNCS, vol. 9665, pp. 1–27. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49890-3_1

[GPSW06] Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: ACM CCS 2006, pp. 89–98. ACM Press (2006)

[Gro06] Groth, J.: Simulation-sound NIZK proofs for a practical language and constant size group signatures. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 444–459. Springer, Heidelberg (2006). https://doi.org/10.1007/11935230_29

[GW09] Gentry, C., Waters, B.: Adaptive security in broadcast encryption systems (with short ciphertexts). In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 171–188. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-01001-9_10

[Hof17] Hofheinz, D.: Adaptive partitioning. In: Coron, J.-S., Nielsen, J.B. (eds.) EUROCRYPT 2017. LNCS, vol. 10212, pp. 489–518. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56617-7_17

[HWL+16] He, K., Weng, J., Liu, J., Liu, J.K., Liu, W., Deng, R.H.: Anonymous identity-based broadcast encryption with chosen-ciphertext security. In: ASIACCS 2016, pp. 247–255. ACM Press (2016)

[KD04] Kurosawa, K., Desmedt, Y.: A new paradigm of hybrid encryption scheme. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 426–442. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-28628-8_26

[KS12] Kiayias, A., Samari, K.: Lower bounds for private broadcast encryption. In: Kirchner, M., Ghosal, D. (eds.) IH 2012. LNCS, vol. 7692, pp. 176–190. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-36373-3_12

[Kur02] Kurosawa, K.: Multi-recipient public-key encryption with shortened ciphertext. In: Naccache, D., Paillier, P. (eds.) PKC 2002. LNCS, vol. 2274, pp. 48–63. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-45664-3_4

[KW15] Kiltz, E., Wee, H.: Quasi-adaptive NIZK for linear subspaces revisited. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9057, pp. 101–128. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46803-6_4

[LOS+10] Lewko, A., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 62–91. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_4

[LPQ12] 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.) PKC 2012. LNCS, vol. 7293, pp. 206–224. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-30057-8_13

[Moh10] Mohassel, P.: A closer look at anonymity and robustness in encryption schemes. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 501–518. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-17373-8_29

[MRV16] Morillo, P., Ràfols, C., Villar, J.L.: The kernel matrix Diffie-Hellman assumption. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10031, pp. 729–758. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53887-6_27

[NNL01] Naor, D., Naor, M., Lotspiech, J.: Revocation and tracing schemes for stateless receivers. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 41–62. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44647-8_3

[OT10] Okamoto, T., Takashima, K.: Fully secure functional encryption with general relations from the decisional linear assumption. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 191–208. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14623-7_11

[Sha84] Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985). https://doi.org/10.1007/3-540-39568-7_5

[SW05] Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005). https://doi.org/10.1007/11426639_27

[Wee10] Wee, H.: Efficient chosen-ciphertext security via extractable hash proofs. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 314–332. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14623-7_17

[Wee16] Wee, H.: Déjà Q: encore! Un petit IBE. In: Kushilevitz, E., Malkin, T. (eds.) TCC 2016. LNCS, vol. 9563, pp. 237–258. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49099-0_9

[YFDL04] Yao, D., Fazio, N., Dodis, Y., Lysyanskaya, A.: ID-based encryption for complex hierarchies with applications to forward security and broadcast encryption. In: ACM CCS 2004, pp. 354–363. ACM Press (2004)