# Compact IBBE and Fuzzy IBE from Simple Assumptions

Junqing Gong[1(✉)], Benoît Libert[1,2(✉)], and Somindu C. Ramanna[3(✉)]

[1] ENS de Lyon, Laboratoire LIP (U. Lyon, CNRS, ENSL, INRIA, UCBL), Lyon, France
{junqing.gong,benoit.libert}@ens-lyon.fr
[2] CNRS, Laboratoire LIP, Lyon, France
[3] Indian Institute of Technology, Kharagpur, India
somindu@cse.iitkgp.ernet.in

**Abstract.** We propose new constructions for identity-based broadcast encryption (IBBE) and fuzzy identity-based encryption (FIBE) in bilinear groups of composite order. Our starting point is the IBBE scheme of Delerablée (Asiacrypt 2007) and the FIBE scheme of Herranz *et al.* (PKC 2010) proven secure under parameterised assumptions called generalised decisional bilinear Diffie-Hellman (GDDHE) and augmented multi-sequence of exponents Diffie-Hellman (aMSE-DDH) respectively. The two schemes are described in the prime-order pairing group. We transform the schemes into the setting of (symmetric) composite-order groups and prove security from two static assumptions (subgroup decision).

The Déjà Q framework of Chase *et al.* (Asiacrypt 2016) is known to cover a large class of parameterised assumptions (dubbed über assumption), that is, these assumptions, when defined in asymmetric composite-order groups, are implied by subgroup decision assumptions in the underlying composite-order groups. We argue that the GDDHE and aMSE-DDH assumptions are not covered by the Déjà Q über assumption framework. We therefore work out direct security reductions for the two schemes based on subgroup decision assumptions. Furthermore, our proofs involve novel extensions of Déjà Q techniques of Wee (TCC 2016-A) and Chase *et al.*

Our constructions have constant-size ciphertexts. The IBBE has constant-size keys as well and guarantees stronger security as compared to Delerablée's IBBE, thus making it the first compact IBBE known to be selectively secure without random oracles under simple assumptions. The fuzzy IBE scheme is the first to simultaneously feature constant-size ciphertexts and security under standard assumptions.

**Keywords:** Identity-based broadcast encryption · Fuzzy IBE
Space efficiency · Simple assumptions


D. Catalano and R. De Prisco (Eds.): SCN 2018, LNCS 11035, pp. 563–582, 2018.
https://doi.org/10.1007/978-3-319-98113-0_30

## 1 Introduction

Identity-based encryption (IBE) [55] is a public-key paradigm where users' private keys are generated by trusted authorities and derived from some easy-to-remember string (like an email address) that serves as a public key so as to simplify key management. Attribute-based encryption (ABE) [36,54] is a powerful extension of IBE where ciphertexts are labeled with a set of descriptive attributes (e.g., "hiring committee", "admin", ...) in such a way that decryption works whenever these attributes satisfy an access policy which is hard-coded in the decryption key.

Functional encryption (FE) [15,54] is an extreme generalization of IBE, where a master private key $SK$ allows deriving sub-keys $SK_F$ associated with functions $F$. Given an encryption $C$ of a message $X$, a sub-key $SK_F$ allows computing $F(X)$ while revealing nothing else about $X$. The message $X = (\mathsf{ind}, M)$ usually consists of an index $\mathsf{ind}$, which is essentially a set of attributes, and a message $M$, which is sometimes called "payload". While the latter is always computationally hidden, the index $\mathsf{ind}$ of a ciphertext may be public or private. Not surprisingly, schemes in the public index setting tend to be significantly more efficient in terms of ciphertext and key sizes.

In the private-index setting, anonymous IBE [10,17] is an example of functional encryption for the equality testing functionality. In the public [36,54] and private-index [39] cases, ABE can be cast as another particular flavour of FE, where private keys are associated with expressive access policies. These primitives provide fine-grained access control [54] or privacy-preserving searches over encrypted data [1,10]. In its key-policy (KP-ABE) flavour, ABE involves private keys associated with a possibly complex Boolean expression $F$ and, if the ciphertext encrypts the message $X = (\mathsf{ind}, M)$, the private key $SK_F$ reveals $M$ if and only if $F(\mathsf{ind}) = 1$. Ciphertext-policy ABE (CP-ABE) schemes proceed the other way around: ciphertexts are labeled with a policy $F$; private keys are associated with an attribute set $\mathsf{ind}$ and decryption succeeds whenever $F(\mathsf{ind}) = 1$.

The usual "collusion-resistance" requirement captures the intuition that no collection of private keys should make it possible to decrypt a ciphertext that none of these keys can individually decrypt. While properly defining the security of FE turns out to be non-trivial [15], the literature usually distinguishes selective adversaries [18] – that have to declare the index of the challenge ciphertext $\mathsf{ind}^\star$ upfront (even before seeing the master public key) – from adaptive adversaries, which can choose $\mathsf{ind}^\star$ after having made a number of private key queries for functions of their choice.

In terms of expressiveness, a major challenge is certainly to efficiently evaluate any polynomial-time-computable function $F$ over encrypted data. While theoretical solutions achieve this goal using the obfuscation machinery [32], practical instantiations of functional encryption are only known for very restricted classes of functions (such as IBE [11,58] or ABE [39]) for the time being.

Even for particular functionalities and selective adversaries, proving security is challenging when we seek to optimise the size of ciphertexts and keys. For example, squeezing many attributes in the same ciphertext component often

comes at the price of larger private keys [4,6] or security proofs under fancy $q$-type assumptions [9,13] (or both). Likewise, short private keys and public parameters [40,51] often entail strong, variable-size assumptions. Eventually, constant-size ciphertexts or keys ("constant" meaning that it only depends on the security parameter and not on the number of adversarial queries or features of the system) often translate into non-constant-size assumptions. In some situations, information theoretic arguments [31] even rule out the possibility of simultaneously achieving constant-size ciphertexts and keys, no matter which assumption is considered.

Here, we restrict ourselves to specific functionalities for which we are interested in proving the security of *compact* schemes under well-studied, constant-size assumptions. By "compact", we mean that ciphertexts can be comprised of a *constant* number of group elements – no matter how many attributes or users are associated with them – without inflating the private key size. In particular, private keys should be no longer than in realisations of the same functionality without short ciphertexts. Finally, we aim at avoiding the caveat of relying on variable-size, $q$-type assumptions, which should notoriously be used with caution [24].

We achieve this goal for two natural extensions of IBE, which are known as *identity-based broadcast encryption* (IBBE) [2,52] and *fuzzy identity-based encryption* (FIBE) [54]. In the former, ciphertexts are encrypted for a list of identities. The latter is an ABE for policies consisting of a single threshold gate: i.e., ciphertexts and private keys both correspond to a set of attributes and decryption succeeds whenever the two sets have a sufficiently large intersection. In fact, IBBE and FIBE can both be seen as special cases of CP-ABE for policies consisting of a single gate: an IBBE is nothing but a CP-ABE for one OR gate, which is implied by FIBE for 1-out-of-$n$ gates. However, considering the two primitives separately allows obtaining shorter private keys in the IBBE case.

### 1.1 Our Contribution

We describe the first IBBE system with a security proof under constant-size assumptions and that simultaneously features constant-size ciphertexts and private keys. In our scheme, only the size of public parameters depends on the maximal number $n$ of receivers per ciphertext. Users' private keys only consist of a single(!) group element while ciphertexts are only longer than plaintexts by 2 elements of a composite-order group. We prove selective security in the standard model under subgroup assumptions [42] in bilinear groups of order $N = p_1p_2p_3$. In comparison, all earlier IBBE realisations with short ciphertexts either incur $O(n)$-size private keys [2,5,14,47] or combine the random oracle model [8] with very *ad hoc* assumptions [26,52] tailored to the result to be proved.

As a second contribution, we extend our IBBE scheme into a fuzzy IBE system with $O(1)$-size ciphertexts and private keys made of $O(\ell)$ group elements, where $\ell$ is the maximal number of attributes per identity. Our FIBE scheme thus asymptotically achieves the same private key size as [54] with the benefit of constant-size ciphertexts, regardless of the number of ciphertext attributes. In

contrast, except [37], previously known KP-ABE systems with short ciphertexts either inflate private keys by a factor $O(\ell)$ [6,7,47,49] or are restricted to small attribute universes [38].

While our constructions rely on composite order groups where pairings are rather expensive to compute [30], they only require two pairing evaluations on behalf of the receiver (and no pairing on the sender's side). Our schemes are proved selectively secure using the Déjà Q technique of Chase and Meiklejohn [22], which was re-used by Wee [62] and refined by Chase *et al.* [23]. A detailed comparison is shown in Table 1. See the full paper [33] for more discussion.

**Table 1.** Comparison among compact IBBE and FIBE. For IBBE, $n$ is the maximum number of recipients; for FIBE, $n$ is the maximum size of attribute set and $\tau$ is the threshold. We use notations—$\mathsf{CT}$: ciphertext; $\mathsf{SK}$: secret key; #dec: cost of decryption; $\mathbb{G}_N$: symmetric pairing group with composite order $N$; $\mathbb{G}_1$, $\mathbb{G}_2$: source groups of an asymmetric pairing group of prime order $p$; [P]: a pairing operation; [M]: scalar multiplication on source groups; aID: adaptive/full security; sID: selective security; na-sID: selective security with non-adaptive key extraction queries; saID: semi-adaptive security; Static: static assumption in $\mathbb{G}_N$; GGM: generic group model; RO: random oracle model.

| | | $\lvert\mathsf{CT}\rvert$ | $\lvert\mathsf{SK}\rvert$ | #dec | Security | Assumption |
|---|---|---|---|---|---|---|
| IBBE | [26]-1 | $\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_2\rvert$ | $\lvert\mathbb{G}_1\rvert$ | $2[\mathrm{P}] + O(n)[\mathrm{M}]$ | sID | GDDHE,RO |
| | [26]-2 | $\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_2\rvert$ | $\lvert\mathbb{G}_1\rvert + \lvert\mathbb{Z}_p\rvert$ | $2[\mathrm{P}] + O(n)[\mathrm{M}]$ | na-sID | O-GDDHE |
| | [52] | $2\lvert\mathbb{G}_1\rvert$ | $\lvert\mathbb{G}_2\rvert$ | $2[\mathrm{P}] + O(n)[\mathrm{M}]$ | aID | GGM,RO |
| | Ours | $2\lvert\mathbb{G}_N\rvert$ | $\lvert\mathbb{G}_N\rvert$ | $2[\mathrm{P}] + O(n)[\mathrm{M}]$ | sID | Static |
| FIBE | [37] | $2\lvert\mathbb{G}_1\rvert$ | $n\lvert\mathbb{G}_1\rvert + n\lvert\mathbb{G}_2\rvert$ | $2[\mathrm{P}] + O(\tau^2 + n)[\mathrm{M}]$ | sID | aMSE-DDH |
| | [4,6] | $2\lvert\mathbb{G}_1\rvert$ | $(n^2 + n)\lvert\mathbb{G}_2\rvert$ | $2[\mathrm{P}] + O(n\tau)[\mathrm{M}]$ | sID | DBDHE |
| | [21] | $2\lvert\mathbb{G}_N\rvert$ | $(n^2 + n)\lvert\mathbb{G}_N\rvert$ | $2[\mathrm{P}] + O(n\tau)[\mathrm{M}]$ | saID | Static |
| | [56] | $17\lvert\mathbb{G}_1\rvert$ | $(6n^2 + 5)\lvert\mathbb{G}_2\rvert$ | $17[\mathrm{P}] + O(n\tau)[\mathrm{M}]$ | saID | DLIN |
| | [7] | $6\lvert\mathbb{G}_N\rvert$ | $(n^2 + 2n + 3)\lvert\mathbb{G}_N\rvert$ | $6[\mathrm{P}] + O(n\tau)[\mathrm{M}]$ | aID | Static |
| | Ours | $2\lvert\mathbb{G}_N\rvert$ | $2n\lvert\mathbb{G}_N\rvert$ | $2[\mathrm{P}] + O(\tau^2 + n)[\mathrm{M}]$ | sID | Static |

### 1.2 Overview of Our Techniques

Our identity-based broadcast encryption scheme is obtained by instantiating (a variant of) Delerablée's IBBE [26] in composite order groups and providing a direct security proof, analogously to Wee's IBE [62]. In prime order groups, Delerablée's construction [26] is proved selectively secure in the random oracle model under a highly non-standard $q$-type assumption, where $q$ simultaneously depends on the number of private key queries and the maximal number of receivers per ciphertext. While this assumption is a special case of the Uber assumption of Boneh, Boyen and Goh [9], it seems to escape the family of assumptions that reduce the constant-size subgroup assumptions via the framework of Chase, Maller and Meiklejohn [23]: in Sect. 3.1, we indeed explain why the results of [23] alone do not immediately guarantee the security of Delerablée's IBBE in

composite order groups.[1] Moreover, even if they did, a direct instantiation of [26] in composite order groups would only be guaranteed to be secure in the random oracle model.[2] In contrast, we give a direct proof of selective security in the standard model.

Just like [26,62], our scheme uses the private key generation technique of the Sakai-Kasahara IBE [53], which computes inversions in the exponent. Letting $\mathbb{G}$ be a cyclic group of order $N = p_1p_2p_3$ with subgroups $\mathbb{G}_{p_i}$ of order $p_i$ for each $i \in \{1,2,3\}$, if $g^\gamma \in \mathbb{G}_{p_1}$ and $G_i = g^{(\alpha^i)} \in \mathbb{G}_{p_1}$ are part of the public parameters, a private key for the identity $\mathsf{id}$ consists of $\mathsf{SK}_{\mathsf{id}} = u^{\gamma/(\alpha+\mathsf{id})} \cdot X_{p_3}$, where $u \in \mathbb{G}_{p_1}$ belongs to the master secret key and $X_{p_3} \in_R \mathbb{G}_{p_3}$. If $S = \{\mathsf{id}_1, \ldots, \mathsf{id}_\ell\}$ denotes the set of authorised receivers, one of the ciphertext components packs their identities into one group element $g^{s \cdot \prod_{\mathsf{id} \in S}(\alpha+\mathsf{id})}$, which can be seen as a randomised version of Nguyen's accumulator [45]. As shown in [26], by introducing $g^{\gamma \cdot s}$ in the ciphertext and blinding the message as $M \oplus \mathsf{H}(e(g,u)^{\gamma \cdot s})$, we can enable decryption by exploiting the divisibility properties of the polynomial $p_S(\alpha) = \prod_{\mathsf{id} \in S}(\alpha + \mathsf{id})$, analogously to [45]. Like the security proof of Wee's IBE [62], our proof proceeds by first introducing $\mathbb{G}_{p_2}$ components in ciphertexts. Then, following the technique of [22], it uses the entropy of $\alpha, \gamma \bmod p_2$ – which are information theoretically hidden by $g^\gamma$ and $G_i = g^{(\alpha^i)}$ – to gradually introduce $\mathbb{G}_{p_2}$ components of the form $g_2^{\sum_{j=1}^k \tilde{\gamma} \cdot r_j \cdot p_S(\alpha_j)/(\alpha_j+\mathsf{id})}$, where $\{r_j\}_{j=1}^k$ are shared by all private keys. At each step, we can increase the number of terms in the exponent so that, when $k$ is sufficiently large, all keys $\mathsf{SK}_{\mathsf{id}}$ have independent random components of order $p_2$. At this point, an information theoretic argument shows that the ciphertext statistically hides the plaintext.

The crucial step of the proof consists of arguing that the newly introduced term in the sum $\sum_{j=1}^k r_j \cdot p_S(\alpha_j)/(\alpha_j + \mathsf{id})$ is statistically independent of the public parameters. At this step, our information theoretic argument differs from Wee's [62] because, in our IBBE system, public parameters contain additional group elements of the form $U_i = u^{\alpha^i} \cdot R_{3,i}$, which inherit $\mathbb{G}_{p_2}$ components that depend on $\sum_{j=1}^k r_j \cdot \alpha_j^i \bmod p_2$, for the same coefficients $r_j \in \mathbb{Z}_{p_2}$ as those showing up in private keys. Since private keys and public key components $\{U_i\}_{i=1}^n$ have correlated semi-functional components[3] that share the same $\{r_j \bmod p_2\}_{j=1}^k$, we have to consistently maintain this correlation at all steps of the sequence of game and argue that, when we reach the final game, the $\mathbb{G}_{p_2}$ components of $\mathsf{SK}_{\mathsf{id}_1}, \ldots, \mathsf{SK}_{\mathsf{id}_q}$ and $\{U_i\}_{i=1}^n$ are uncorrelated in the adversary's

[1] We believe our arguments showing that the assumptions under question are not covered by the Déjà Q framework are sufficient. Also, we do not know if there exist other parameterised assumptions in this class that could possibly be used to prove security of the IBBE and FIBE schemes.

[2] Alternatively, the scheme of [26] can be proved secure in the standard model if the adversary also announces all its private keys queries (in addition to the target set of identities) before seeing the public parameters.

[3] The proof of Wee's broadcast encryption [62, Sect. 4] has a similar correlation between the $\mathbb{G}_{p_2}$ components of private keys and public parameters but, in the final step, the statistical argument involved simpler-to-analyse Vandermonde matrices.

view. In Wee's constructions [62], this is done by arguing that matrices of the form $(\alpha_j^i)_{i,j\in[q]}$ or $\big(1/(\alpha_j+\mathsf{id}_i)\big)_{i,j}$ are invertible. Here, we are presented with more complex square matrices that involve the two kinds of entries and also depend on the polynomial $p_{S^\star}(\alpha)=\prod_{\mathsf{id}\in S^\star}(\alpha+\mathsf{id})$, where $S^\star$ is the set of the target identities. More precisely, these matrices contain sub-matrices of the form $\big(p_{S^\star}(\alpha_i)/(\alpha_i+\mathsf{id}_j)\big)_{i,j}$, where $\mathsf{id}_j$ denotes the $j$-th private key query. We use the property that the overall square matrices are invertible over $\mathbb{Z}_{p_2}$ as long as none of the first-degree $(\alpha+\mathsf{id}_j)$ divides $p_{S^\star}(\alpha)$ (i.e., $\mathsf{id}_j\notin S^\star$ for all private key queries $\mathsf{id}_j$). When this is the case, we are guaranteed that the $\mathbb{G}_{p_2}$ components of ciphertexts, private keys and public parameters are i.i.d. in the adversary's view.

Our fuzzy IBE construction is an adaptation of the system described by Herranz, Laguillaumie and Ràfols [4,37] in prime order groups, which is itself inspired by the dynamic threshold encryption primitive of Delerablée and Pointcheval [27] and relies on a similarly strong assumption. The FIBE system of [37] modifies [26,27] by randomizing the generation of private keys. In our construction, private keys for an attribute set $\{\mathsf{id}_1,\ldots,\mathsf{id}_\ell\}$ similarly consist of

$$\big(K_i=u^{\frac{\gamma}{\alpha+\mathsf{id}_i}}\cdot X_{3,i}\big)_{i=1}^{\ell},\qquad \big(K_i'=u^{\alpha^i}\cdot X_{3,i}'\big)_{i=1}^{n-1},\qquad K_0=u\cdot u_0\cdot X_{3,0},$$

where $u\in_R\mathbb{G}_{p_1}$ and $X_{3,i}\in_R\mathbb{G}_{p_3}$ are freshly chosen for each key and $u_0\in\mathbb{G}_{p_1}$ is a master secret key component which is committed via $e(g,u_0)^\gamma$ in the master public key. Intuitively, the public parameters $u_0^{\alpha^i}\cdot R_{3,i}$ of Delerablée's IBBE are now replaced by similar-looking private key components $K_i'=u^{\alpha^i}\cdot X_{3,i}'$ for random $u\in_R\mathbb{G}_1$ that are used in $K_0$ to blind the master secret key $u_0$ (collusion-resistance is ensured by the fact that distinct keys involve fresh randomizers $u$).

Due to the strong structural similarity, the proof for the selective security of our fuzzy IBE can be viewed as an extension of that for our IBBE system. From the viewpoint of reduction, the fresh $u\in\mathbb{G}_{p_1}$ in each secret key allows us to correspond each secret key to a fresh IBBE instance and analyse them in an independent fashion. In particular, by considering $K_i$ as $\mathsf{SK}_{\mathsf{id}_i}$ and $K_i'$ as $U_i$, we can apply the proof method of our IBBE to introduce independent random $\mathbb{G}_{p_2}$ components in all these components and $K_0$ (with $u_0\cdot X_{3,0}$). As discussed earlier, the core step is again to argue the invertibility of a matrix of some special form for each secret key. Although the matrices we are considering now look like those for the IBBE system, the situation is actually more complex. More specifically, the matrices contain sub-matrices of the form $(p_{S^\star,\tau^\star}(\alpha_i)/(\alpha_i+\mathsf{id}_j))_{i,j}$ where $p_{S^\star,\tau^\star}(\alpha)=\prod_{\mathsf{id}\in S^\star}(\alpha+\mathsf{id})\cdot\prod_{i\in[\delta]}(\alpha+d_i)$ where $S^\star$ is the set for the target fuzzy identity, $(d_i)_i$ is a set of dummy identities and $\delta$ depends on the target threshold $\tau^*$. Unlike the IBBE case, there can be an $\mathsf{id}_j\in\{\mathsf{id}_1,\ldots,\mathsf{id}_\ell\}$ such that $\mathsf{id}_j\in S^\star$ so that $(\alpha+\mathsf{id}_j)$ divides $p_{S^\star,\tau^\star}(\alpha)$ in the FIBE case. This prevents us from directly applying our previous result on the matrices. Instead, we will prove the property that these matrices are still invertible as long as the number of such $\mathsf{id}_j$ do not exceed the target threshold $\tau^*$. Inspired by the recent proof for IBE in the multi-instance setting [19], we can in fact change the distributions of all secret keys *independently* but *simultaneously* using the random self-reducibility of decisional

subgroup assumptions. Once we have independent random $\mathbb{G}_{p_2}$ component in $K_0$ in each secret key, we then introduce semi-functional component (in $\mathbb{G}_{p_2}$) for the master secret key component $u_0$ and show that it will be hidden by the random $\mathbb{G}_{p_2}$ component in $K_0$. This means the semi-functional component of $u_0$ will only appear in the challenge ciphertext which is adequate for proving the selective security of our fuzzy IBE system.

### 1.3 Related Work

Broadcast encryption was introduced by Fiat and Naor [29] and comes either in combinatorial [43] or algebraic flavors [13,34,40,44,59]. One of the most appealing tradeoffs was given in the scheme of Boneh, Gentry and Waters [13], which features short ciphertexts and private keys but linear-size public keys in the total number of users. While its security was initially proved under a parameterised assumption, recent extensions [23,62] of the Déjà Q framework [22] showed how to prove the security (against static adversaries) of its composite-order-group instantiations under constant-size subgroup assumptions. Boneh *et al.* suggested a variant [16] of the BGW scheme [13] with polylogarithmic complexity in all metrics using multi-linear maps. Unfortunately, the current status of multi-linear maps does not enable secure instantiations of [16] for now (see, e.g., [25]).

Identity-based broadcast encryption was formally defined by Abdalla, Kiltz and Neven [2] and independently considered by Sakai and Furukawa [52]. One of the salient advantages of IBBE over traditional public-key broadcast encryption is the possibility of accommodating an exponential number of users with polynomial-size public parameters. IBBE was recently used [28] in the design of efficient 0-RTT key exchange protocols with forward secrecy. Abdalla *et al.* [2] gave a generic construction with short ciphertexts and private keys of size $O(n^2)$, where $n$ is the maximal number of receivers. Sakai and Furukawa [52] suggested a similar construction to [26] with security proofs in the generic group and random oracle model. Boneh and Hamburg [14] obtained a system with $O(1)$-size ciphertexts and $O(n)$-size keys. Using the Déjà Q technique, Chen *et al.* [20] described an identity-based revocation mechanism [40] with short ciphertexts and private keys under constant-size assumptions. The aforementioned constructions were all only proven secure against selective adversaries. Gentry and Waters [34] put forth an adaptively secure construction based on $q$-type assumptions while Attrapadung and Libert [5] showed a fully secure variant of [14] under simple assumptions. To our knowledge, the only IBBE realisations that simultaneously feature constant-size ciphertexts and private keys are those of [26,52], which require highly non-standard assumptions and the random oracle model. As mentioned by Derler *et al.* [28], the short ciphertexts and private keys of Delerablée's scheme [26] make it interesting to instantiate their generic construction of Bloom Filter Encryption, which in turn implies efficient 0-RTT key exchange protocols. Until this work, even for selective adversaries, it has been an open problem to simultaneously achieve short ciphertext and private keys without resorting to variable-size assumptions.

Attribute-based encryption was first considered in the seminal paper by Sahai and Waters [54]. Their fuzzy IBE primitive was later extended by Goyal *et al.* [36] into more expressive forms of ABE, where decryption is possible when the attribute set of the ciphertext satisfies a more complex Boolean formula encoded in the private key. After 2006, a large body of work was devoted to the design of adaptively secure [7,41,46–49,57] and more expressive ABE systems [12,35, 40,50,60,61]. In contrast, little progress has been made in the design of ABE schemes with short ciphertexts. The first reasonably expressive ABE systems with constant-size ciphertexts were given in [4,6,37] under $q$-type assumptions. The solution of Herranz *et al.* [37] is a fuzzy IBE (i.e., a CP-ABE system for one threshold gate) with private keys of size $O(n)$ where $n$ is the maximal number of attributes per ciphertext. The more expressive KP-ABE systems of [4,6] support arbitrary Boolean formulas, but enlarge the private keys of [36] by a factor $n$. The construction of [38, Sect. 3.4] eliminates the upper bound on the number of ciphertext attributes, but lengthens private keys by a factor $|U|$, where $U$ is the universe of attributes. Several follow-up works improved upon [6] by proving security under simple assumptions [21,56] or achieving full security [7]. However, all known KP-ABE schemes with short ciphertexts under simple assumptions suffer from similarly large private keys. While our scheme only supports one threshold gate, it turns out to be the first solution with short ciphertexts under simple assumptions that avoids blowing up private keys by a factor $O(n)$.

## 2 Preliminaries

NOTATION. We write $x_1, \ldots, x_k \xleftarrow{R} \mathcal{X}$ to indicate that $x_1, \ldots, x_k$ are sampled independently and uniformly from the set $\mathcal{X}$. For a PPT algorithm $\mathcal{A}$, $y \xleftarrow{R} \mathcal{A}(x)$ means that $y$ is chosen according to the output distribution of $\mathcal{A}$ on input $x$. For integers $a < b$, $[a, b]$ denotes the set $\{x \in \mathbb{Z} : a \leq x \leq b\}$ and we let $[b] = [1, b]$. If $\mathbb{G}$ is a cyclic group, $\mathbb{G}^{\times}$ denotes the set of generators of $\mathbb{G}$.

### 2.1 Composite-Order Pairings and Hardness Assumptions

A (symmetric) composite-order pairing ensemble generator $\mathsf{GroupGen}()$ is an algorithm that inputs a security parameter $\eta$ and an integer $m$ and returns an $(m+3)$-tuple $\mathcal{G} = (p_1, \ldots, p_m, \mathbb{G}, \mathbb{G}_T, e)$ where $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic groups of order $N = p_1 \cdots p_m$ (a square-free, hard-to-factor integer) and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a non-degenerate and efficiently computable bilinear map. The primes are chosen so that $p_i > 2^{\eta}$ for $i \in \{1, 2, \ldots, m\}$. We will use hardness assumptions which require the factorisation of $N$ to remain hidden. Given $\mathcal{G} = (p_1, \ldots, p_m, \mathbb{G}, \mathbb{G}_T, e)$, let $\mathcal{G}_{\mathrm{pub}} = (N, \mathbb{G}, \mathbb{G}_T, e)$ denote the public description of $\mathcal{G}$ where $N = p_1 \cdots p_m$ and we assume that $\mathbb{G}, \mathbb{G}_T$ contain respective generators (of the full groups). Letting $\mathbb{G}_{p_i}$ be the subgroup of order $p_i$ of $\mathbb{G}$, we denote elements of $\mathbb{G}_{p_i}$ with subscript $i$ for $i \in [m]$. We now describe decisional subgroup (DS) assumptions w.r.t. $(\mathcal{G} = (p_1, p_2, p_3, \mathbb{G}, \mathbb{G}_T, e)) \longleftarrow \mathsf{GroupGen}(\eta, 3)$, which is stated in terms of

two distributions: $\mathcal{D}, T_1$ and $\mathcal{D}, T_2$. We define $\mathsf{Adv}^{\mathscr{B}}_{\mathcal{G},\mathrm{DS}}(\eta) = |\Pr[\mathscr{B}(\mathcal{D}, T_1) = 1] - \Pr[\mathscr{B}(\mathcal{D}, T_2) = 1]|$ to be the advantage of a distinguisher $\mathscr{B}$ against DS. We now describe $\mathcal{D}, T_1, T_2$ for the assumptions we use.

**Assumption DS1.** Pick generators $g_1 \xleftarrow{R} \mathbb{G}_{p_1}$ and $g_3 \xleftarrow{R} \mathbb{G}_{p_3}$. Define $\mathcal{D} = (\mathcal{G}_{\mathrm{pub}}, g_1, g_3)$, $T_1 \xleftarrow{R} \mathbb{G}_{p_1}$ and $T_2 \xleftarrow{R} \mathbb{G}_{p_1 p_2}$. DS1 holds if for all PPT $\mathscr{B}$, $\mathsf{Adv}^{\mathscr{B}}_{\mathcal{G},\mathrm{DS1}}(\eta)$ is negligible in $\eta$.

**Assumption DS2.** Pick $g_1 \xleftarrow{R} \mathbb{G}_{p_1}$, $g_3 \xleftarrow{R} \mathbb{G}_{p_3}$, $h_{12} \xleftarrow{R} \mathbb{G}_{p_1 p_2}$ and $h_{23} \xleftarrow{R} \mathbb{G}_{p_2 p_3}$. Define $\mathcal{D} = (\mathcal{G}_{\mathrm{pub}}, g_1, g_3, h_{12}, h_{23})$, $T_1 \xleftarrow{R} \mathbb{G}_{p_1 p_3}$ and $T_2 \xleftarrow{R} \mathbb{G}_{p_1 p_2 p_3}$. The DS2 assumption holds if for all PPT $\mathscr{B}$, $\mathsf{Adv}^{\mathscr{B}}_{\mathcal{G},\mathrm{DS2}}(\eta)$ is negligible in $\eta$.

### 2.2 Identity-Based Broadcast Encryption (IBBE)

**Definition 1 (IBBE).** *An IBBE scheme is defined by probabilistic algorithms* Setup, KeyGen, Encrypt *and* Decrypt. *The identity space is denoted by* $\mathcal{I}$ *and the message space is denoted by* $\mathcal{M}$.

$\mathsf{Setup}(1^\lambda, 1^n)$**:** *Takes as input a security parameter* $\lambda$, *the maximum number* $n$ $(= \mathsf{poly}(\lambda))$ *of recipient identities in a broadcast and generates the public parameters* PP *and the master secret* MSK. *The algorithm also defines the identity space* $\mathcal{I}$ *and message space* $\mathcal{M}$.

$\mathsf{KeyGen}(\mathsf{MSK}, \mathsf{id})$**:** *Inputs an identity* id *and* MSK*; outputs a key* $\mathsf{SK}_{\mathsf{id}}$ *for* id.

$\mathsf{Encrypt}(\mathsf{PP}, S \subseteq \mathcal{I}, m \in \mathcal{M})$**:** *Takes as input the public parameters and a set of identities* $S$ *intended to receive the message* $m$. *If* $|S| \leq n$, *the algorithm outputs the ciphertext* CT.

$\mathsf{Decrypt}(\mathsf{PP}, S, \mathsf{CT}, \mathsf{id}, \mathsf{SK}_{\mathsf{id}})$**:** *Inputs* PP, *a set* $S = \{\mathsf{id}_1, \ldots, \mathsf{id}_\ell\}$, *an identity* id, *a secret key* $\mathsf{SK}_{\mathsf{id}}$ *for* id, *a ciphertext* CT *and outputs a message* $m' \in \mathcal{M}$ *if* $\mathsf{id} \in S$ *and otherwise outputs* $\perp$.

**Correctness.** The IBBE scheme satisfies correctness if, for all sets $S \subseteq \mathcal{I}$ with $|S| \leq n$, for all identities $\mathsf{id}_i \in S$, for all messages $m \in \mathcal{M}$, if $(\mathsf{PP}, \mathsf{MSK}) \xleftarrow{R} \mathsf{Setup}(1^\lambda, 1^n)$, $\mathsf{SK}_{\mathsf{id}_i} \xleftarrow{R} \mathsf{KeyGen}(\mathsf{MSK}, \mathsf{id}_i)$ and $\mathsf{CT} \xleftarrow{R} \mathsf{Encrypt}(\mathsf{PP}, S, m)$, then we have $\Pr[m = \mathsf{Decrypt}(\mathsf{PP}, S, \mathsf{CT}, \mathsf{id}_i, \mathsf{SK}_{\mathsf{id}_i})] = 1$.

**Definition 2 (IBBE Security).** *An IBBE system* $\mathcal{IBBE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ *provides selective security if no PPT adversary* $\mathscr{A}$ *has non-negligible advantage in the following game.*

**Initialise:** $\mathscr{A}$ *commits to a target set of identities* $S^* = \{\mathsf{id}_1^*, \ldots, \mathsf{id}_{\ell^*}^*\}$.

**Setup:** *The challenger runs the* Setup *algorithm of* $\mathcal{IBBE}$ *and gives* PP *to* $\mathscr{A}$.

**Key Extraction Phase 1:** $\mathscr{A}$ *makes key extraction queries. For a query on an identity vector* id *such that* $\mathsf{id} \notin S^*$, *the challenger runs* $\mathcal{IBBE}$.KeyGen *algorithm and responds with a key* $\mathsf{SK}_{\mathsf{id}}$.

**Challenge:** *$\mathscr{A}$ provides two messages $m_0, m_1$. The challenger chooses a bit $\beta$ uniformly at random from $\{0,1\}$, computes $\mathsf{CT}^* \xleftarrow{R} \mathcal{IBBE}.\mathsf{Encrypt}(\mathsf{PP}, S^*, m_\beta)$ and returns $\mathsf{CT}^*$ to $\mathscr{A}$.*

**Key Extraction Phase 2:** *$\mathscr{A}$ makes more key extraction queries with the restriction that it cannot query a key for any identity in $S^*$.*

**Guess:** *$\mathscr{A}$ outputs a bit $\beta'$. If $\beta = \beta'$, then $\mathscr{A}$ wins the game. The adversary $\mathscr{A}$'s advantage is given by the distance $\mathsf{Adv}^{\mathscr{A}}_{\mathcal{IBBE},\mathsf{sid\text{-}cpa}}(\lambda) = |\Pr[\beta = \beta'] - 1/2|$.*

### 2.3 Fuzzy Identity-Based Encryption (FIBE)

**Definition 3 (FIBE).** *A fuzzy IBE scheme is defined by probabilistic algorithms –* Setup, KeyGen, Encrypt *and* Decrypt. *The identity space is denoted by $\mathcal{I}$ and the message space is denoted by $\mathcal{M}$.*

$\mathsf{Setup}(1^\lambda, 1^n)$**:** *Takes as input a security parameter $\lambda$, the maximum size $n$ $(= \mathsf{poly}(\lambda))$ of sets associated with ciphertexts and generates the public parameters* PP *and the master secret* MSK. *The algorithm also defines the identity space $\mathcal{I}$ and message space $\mathcal{M}$.*

$\mathsf{KeyGen}(\mathsf{MSK}, S \subseteq \mathcal{I})$**:** *Inputs a set $S$ and* MSK*; outputs a secret key $\mathsf{SK}_S$ for $S$.*

$\mathsf{Encrypt}(\mathsf{PP}, S \subseteq \mathcal{I}, \tau, m \in \mathcal{M})$**:** *Takes as input the public parameters* PP*, a set of identities $S$ along with a threshold $\tau$ and a message $m$. If $\tau \leq |S| \leq n$, the algorithm outputs the ciphertext $\mathsf{CT}_{S,\tau}$.*

$\mathsf{Decrypt}(\mathsf{PP}, S, \tau, \mathsf{CT}_{S,\tau}, S', \mathsf{SK}_{S'})$**:** *This algorithm inputs the public parameters* PP*, a set $S \subseteq \mathcal{I}$ with a threshold $\tau$ and a ciphertext $\mathsf{CT}_{S,\tau}$ associated with them, another set $S' \subseteq \mathcal{I}$ and its corresponding secret key $\mathsf{SK}_{S'}$, outputs a message $m' \in \mathcal{M}$ if $|S \cap S'| \geq \tau$ and $\perp$ otherwise.*

**Correctness.** The FIBE scheme is correct if, for all sets $S \subseteq \mathcal{I}$, all thresholds $\tau \leq |S| \leq n$, all $S' \in \mathcal{I}$ satisfying $|S \cap S'| \geq \tau$, all $m \in \mathcal{M}$, when $(\mathsf{PP}, \mathsf{MSK}) \xleftarrow{R} \mathsf{Setup}(1^\lambda, 1^n)$, $\mathsf{SK}_{S'} \xleftarrow{R} \mathsf{KeyGen}(\mathsf{MSK}, S')$ and $\mathsf{CT}_{S,\tau} \xleftarrow{R} \mathsf{Encrypt}(\mathsf{PP}, S, \tau, m)$, then $\Pr[m = \mathsf{Decrypt}(\mathsf{PP}, S, \tau, \mathsf{CT}_{S,\tau}, S', \mathsf{SK}_{S'})] = 1$.

**Definition 4 (FIBE Security).** *A FIBE system $\mathcal{FIBE}$ =* (Setup, KeyGen, Encrypt, Decrypt) *provides selective security if no PPT adversary $\mathscr{A}$ has non-negligible advantage in the following game.*

**Initialise:** *$\mathscr{A}$ commits to a target set $S^* \subseteq \mathcal{I}$ and threshold $\tau^*$ satisfying $\tau^* \leq |S^*| \leq n$.*

**Setup:** *The challenger runs the* Setup *algorithm of $\mathcal{FIBE}$ and gives* PP *to $\mathscr{A}$.*

**Key Extraction Phase 1:** *$\mathscr{A}$ makes a number of key extraction queries. For a query on $S \subseteq \mathcal{I}$ such that $|S^* \cap S| < \tau^*$, the challenger runs $\mathsf{SK}_S \leftarrow \mathcal{FIBE}.\mathsf{KeyGen}$ and outputs $\mathsf{SK}_S$.*

**Challenge:** *$\mathscr{A}$ provides two messages $m_0, m_1$. The challenger chooses $\beta \xleftarrow{R} \{0,1\}$, computes $\mathsf{CT}^* \xleftarrow{R} \mathcal{FIBE}.\mathsf{Encrypt}(\mathsf{PP}, S^*, \tau^*, m_\beta)$ and returns $\mathsf{CT}^*$ to $\mathscr{A}$.*

**Key Extraction Phase 2:** *$\mathscr{A}$ makes more key extraction queries with the restriction that it cannot query a key for any set $S$ such that $|S^* \cap S| \geq \tau^*$.*

**Guess:** *$\mathscr{A}$ outputs a bit $\beta'$. We say $\mathscr{A}$ wins the game if $\beta = \beta'$. The advantage of $\mathscr{A}$ in winning the* sid-cpa *game is defined to be $\mathsf{Adv}^{\mathscr{A}}_{\mathcal{FIBE},\mathsf{sid\text{-}cpa}}(\lambda) = |\Pr[\beta = \beta'] - 1/2|$.*

## 3 Compact IBBE from Subgroup Decision Assumptions

This section describes our IBBE scheme with short ciphertexts and keys. The structure is similar to Delerablée's IBBE [26] in asymmetric prime-order groups.

### 3.1 Déjà Q Framework and Its Implications on Delerablée's IBBE

The scheme proposed by Delerablée in [26] is based on prime-order asymmetric pairings and offers constant-size ciphertexts and keys. However, its proof of security relies on random oracles and a parameterised assumption called generalised decisional Diffie-Hellman exponent (GDDHE) with instances containing $O(q+n)$ group elements. A scheme/proof without random oracles is also suggested but at the cost of an interactive GDDHE-like assumption and a more restrictive security definition (called IND-na-sID-CPA) in which the adversary has to commit to the identities for key extract queries during the initialisation phase (in addition to the challenge identity set).

It is natural to ask whether the scheme can be lifted to the composite-order setting and proved secure based on subgroup decision assumptions via the Déjà Q framework [22,23]. That is, we ask whether the Uber assumption in asymmetric composite-order bilinear groups defined in [23] covers the GDDHE assumption or not? The answer is negative. To see why, let us take a closer look at the Uber assumption of [23] and the (asymmetric) GDDHE-assumption. For clarity, we avoid formal descriptions of assumptions and other details.

**Uber Assumption** [23]**.** Assume $\mathcal{G} = (N, p_1, p_2, p_3, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$ be an asymmetric composite-order pairing group. Let $R(\boldsymbol{x}), S(\boldsymbol{x}), V(\boldsymbol{x})$ denote sets of polynomials in $n$ variables $\boldsymbol{x} = (x_1, \ldots, x_n)$ and let $z(\boldsymbol{x})$ be a polynomial in $\boldsymbol{x}$. Let $g$ be a generator of $\mathbb{G}_1$ and $h, \hat{h}$ be two independent generators of $\mathbb{G}_2$. The uber assumption states that given

$$g, \hat{h}, g^{R(\boldsymbol{x})}, h^{S(\boldsymbol{x})}, e(g,h)^{V(\boldsymbol{x})}, T$$

it is hard to decide if $T = e(g,\hat{h})^{z(\boldsymbol{x})}$ or $T \in_R \mathbb{G}_T$. It is known [23] that the uber assumption is implied by constant-size subgroup decision assumptions in $\mathbb{G}_1$ and $\mathbb{G}_2$ if $R(\boldsymbol{x}), z(\boldsymbol{x})$ are linearly independent along other requirements (see [23, Proposition 3.9] for a formal statement).

In order to simplify our analysis, we may let $\hat{h}^{\delta} = h$ for an independent exponent $\delta \xleftarrow{R} \mathbb{Z}_N$ and re-state the uber assumption as: given

$$g, \hat{h}, g^{R(\boldsymbol{x})}, \hat{h}^{\delta \cdot S(\boldsymbol{x})}, e(g,\hat{h})^{\delta \cdot V(\boldsymbol{x})}, T$$

it is hard to decide if $T = e(g,\hat{h})^{z(\boldsymbol{x})}$ or $T \in_R \mathbb{G}_T$. Here, $\delta \cdot S(\boldsymbol{x}) = \{\delta \cdot s(\boldsymbol{x}) : s \in S(\boldsymbol{x})\}$ and $\delta \cdot V(\boldsymbol{x}) = \{\delta \cdot v(\boldsymbol{x}) : v \in V(\boldsymbol{x})\}$. We highlight that the Déjà Q framework in [23] requires the polynomials in the exponents of $\hat{h}$ to be in the form of $\delta \cdot \mathsf{poly}(\boldsymbol{x})$ with an independent $\delta$.

**Déjà Q Framework Does Not Cover GDDHE Assumption** [26]**.** Let an asymmetric prime-order pairing configuration $\mathcal{G} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$. Let $g_0, h_0$ be the respective generators of $\mathbb{G}_1, \mathbb{G}_2$. Pick $k, \gamma \xleftarrow{R} \mathbb{Z}_p$ and let $f, g$ be two co-prime polynomials with pairwise distinct roots of respective orders $q, n$. The GDDHE assumption states that given

$$g_0, g_0^{\gamma}, g_0^{\gamma^2}, \ldots, g_0^{\gamma^{q-1}}, g_0^{\gamma f(\gamma)}, g_0^{k\gamma f(\gamma)}, \qquad h_0, h_0^{\gamma}, h_0^{\gamma^2}, \ldots, h_0^{\gamma^{2n}}, h_0^{kg(\gamma)},$$

along with $T \in \mathbb{G}_T$, it is hard to determine whether $T = e(g_0, h_0)^{kf(\gamma)}$ or $T \in_R \mathbb{G}_T$.

As a direct attempt to put GDDHE into the Déjà Q framework, we can let $g = g_0$ and $\hat{h} = h_0$. This means we are considering $\boldsymbol{x} = (\gamma, k)$ and

$$z(\gamma, k) = kf(\gamma),\ V = \emptyset,\ R(\gamma, k) = \{1, \gamma, \gamma^2, \ldots, \gamma^{q-1}, \gamma f(\gamma), k\gamma f(\gamma)\}.$$

In this case, polynomials in the exponents of $\hat{h}$ include $\{1, \gamma, \gamma^2, \ldots, \gamma^{2n}, kg(\gamma)\}$. Since both $\gamma$ and $k$ has appeared in $z(\boldsymbol{x})$ and $R(\boldsymbol{x})$, there's no means to write these polynomials in the form of $\delta \cdot \mathsf{poly}(\boldsymbol{x})$ with an independent variable $\delta$.

With our current choice of $g$, all polynomials in the exponents of $g$ fit the Déjà Q framework quite well. To get around this problem, we try another definition of $\hat{h}$. The best choice can be setting $\hat{h} = h_0^k$, $\boldsymbol{x} = \gamma$ and $z(\gamma) = f(\gamma)$. The basic idea is to set $\delta = k^{-1}$. However, the polynomials in the exponents of $\hat{h}$ become

$$k^{-1}, k^{-1} \cdot \gamma, k^{-1} \cdot \gamma^2, \ldots, k^{-1} \cdot \gamma^{2n}, g(\gamma)$$

where the last polynomial is still in the wrong form and we can not publish $\hat{h}$ itself this time. Even worse, $\delta$ will also appear in the exponent of $g = g_0$ since the input to the adversary contains $g^{k\gamma f(\gamma)}$ (in the original assumption) which will become $g^{\delta^{-1}\gamma f(\gamma)}$ in the current setting. We can make this argument more general. If we want to borrow $\delta$ from $kf(\gamma)$, which seems to be the unique random source we can use in the challenge, it will finally appear (in some form) in the term $g^{k\gamma f(\gamma)}$. Therefore, the Déjà Q transform fails.

In this forthcoming sections, instead of trying to reduce subgroup decision to the GDDHE, we give direct security reductions (via Déjà Q techniques) for constructions in composite-order groups (similar to [26]) from subgroup decision assumptions. Our construction has constant-size ciphertexts and keys and is selectively secure under the static subgroup decision assumptions, thus achieving a stronger security guarantee as compared to [26].

### 3.2 Construction

We now describe the construction $\mathcal{IBBE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Encrypt}, \mathsf{Decrypt})$.

$\mathsf{Setup}(1^\lambda, 1^n)$**:** Let $\mathcal{M} = \{0,1\}^\rho$ where $\rho \in \mathsf{poly}(\lambda)$. Generate a composite-order pairing ensemble $(\mathcal{G} = (p_1, p_2, p_3, \mathbb{G}, \mathbb{G}_T, e)) \longleftarrow \mathsf{GroupGen}(\rho + 2\lambda, 3)$. Set $N = p_1 p_2 p_3$ and $\mathcal{I} = \mathbb{Z}_N$. Pick generators $g, u \xleftarrow{\mathrm{R}} \mathbb{G}_{p_1}^\times$ and $g_3 \xleftarrow{\mathrm{R}} \mathbb{G}_{p_3}^\times$. Sample $R_{3,i} \xleftarrow{\mathrm{R}} \mathbb{G}_{p_3}$ for $i \in [n]$ using $g_3$. Also, choose $\alpha, \gamma \xleftarrow{\mathrm{R}} \mathbb{Z}_N$. Let $\mathsf{H} : \mathbb{G}_T \to \{0,1\}^\rho$ be a universal hash function with output length $\rho$. Define the master secret as $\mathsf{MSK} = (u, \alpha, \gamma, g_3)$ while the public parameters consist of

$$\mathsf{PP} = \big(\mathcal{G}_{\mathrm{pub}},\ g,\ g^\gamma,\ (G_i = g^{\alpha^i},\ U_i = u^{\alpha^i} \cdot R_{3,i})_{i=1}^n,\ e(g,u)^\gamma,\ \mathsf{H}\big).$$

$\mathsf{KeyGen}(\mathsf{MSK}, \mathsf{id})$**:** Pick $X_3 \xleftarrow{\mathrm{R}} \mathbb{G}_{p_3}$ (using generator $g_3$) and generate the key for identity $\mathsf{id}$ as

$$\mathsf{SK}_{\mathsf{id}} = u^{\frac{\gamma}{\alpha + \mathsf{id}}} \cdot X_3.$$

$\mathsf{Encrypt}(\mathsf{PP}, S = \{\mathsf{id}_1, \ldots, \mathsf{id}_\ell\}, M)$**:** To encrypt $M \in \{0,1\}^\rho$ for the set $S$, expand the polynomial $p_S(x) = \prod_{i=1}^{\ell}(x + \mathsf{id}_i) = \sum_{j=0}^{\ell} c_j x^j \in \mathbb{Z}_N[x]$. Choose $s \xleftarrow{R} \mathbb{Z}_N$ and output

$$\mathsf{CT} = \big(C_0 = M \oplus \mathsf{H}(e(g,u)^{s\gamma}),\ C_1 = g^{s\gamma},\ C_2 = \Big(g^{c_0} \cdot \textstyle\prod_{j=1}^{\ell} G_j^{c_j}\Big)^s = g^{s \cdot p_S(\alpha)}\big).$$

$\mathsf{Decrypt}(\mathsf{PP}, S, \mathsf{CT}, \mathsf{id}, \mathsf{SK}_{\mathsf{id}})$**:** If $\mathsf{id} \notin S$, return $\perp$. Otherwise, $p_S(x)/(x + \mathsf{id}) = p_{S \setminus \{\mathsf{id}\}}(x) = \sum_{i=0}^{\ell-1} z_i x^i$ is a polynomial, where $z_0 = \prod_{\mathsf{id}_i \in S \setminus \{\mathsf{id}\}} \mathsf{id}_i$. Output $M = C_0 \oplus \mathsf{H}\big((A_2/A_1)^{1/z_0}\big)$, where

$$A_1 = e(C_1, \prod_{j=1}^{\ell-1} U_j^{z_j}) = e(g^{s\gamma}, u^{p_{S\setminus\{\mathsf{id}\}}(\alpha) - z_0}) = e(g,u)^{s\gamma(p_{S\setminus\{\mathsf{id}\}}(\alpha) - z_0)},$$

$$A_2 = e(C_2, \mathsf{SK}_{\mathsf{id}}) = e(g^{s p_S(\alpha)}, u^{\frac{\gamma}{\alpha+\mathsf{id}}} \cdot X_3) = e(g,u)^{s\gamma p_{S\setminus\{\mathsf{id}\}}(\alpha)}.$$

The correctness of the scheme follows from the divisibility properties of $p_S(x)$ and is easy to verify.

### 3.3 Proof of Security

We give the following theorem and refer to the full version [33] for the proof.

**Theorem 1.** *For any adversary $\mathscr{A}$ attacking $\mathcal{IBBE}$ in the* sid-cpa *model making at most $q$ key extraction queries, there exist algorithms $\mathscr{B}_1, \mathscr{B}_2$ such that*

$$\mathsf{Adv}^{\mathscr{A}}_{\mathcal{IBBE},\mathsf{sid\text{-}cpa}}(\lambda) \le 2 \cdot \mathsf{Adv}^{\mathscr{B}_1}_{\mathcal{G},\mathrm{DS1}}(\lambda) + (q+n+2) \cdot \mathsf{Adv}^{\mathscr{B}_2}_{\mathcal{G},\mathrm{DS2}}(\lambda) + \frac{(q+n+1)^2}{p_2} + \frac{1}{p_2} + \frac{1}{2^\lambda}.$$

## 4 Fuzzy IBE with Short Ciphertexts

We now present a fuzzy IBE scheme obtained by transposing the prime-order construction of Herranz *et al.* [4,37] to composite order groups. The security of their scheme relies on the augmented multi-sequence of exponents decisional Diffie-Hellman (aMSE-DDH) assumption. As in Sect. 3, we start with an explanation of why this assumption is not covered by the Uber assumption of [23].

**Déjà Q Framework Does Not Cover aMSE-DDH Assumption** [4,37]**.** Let an asymmetric prime-order pairing configuration $\mathcal{G} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$. We describe an asymmetric version of the $(\ell, m, t)$-aMSE-DDH assumption.[4] With a length-$(\ell + m)$ vector $\boldsymbol{y} = (y_1, \ldots, y_{l+m})$, define functions $f(Y) = \prod_{i=1}^{\ell}(Y + y_i)$ and $g(Y) = \prod_{i=\ell+1}^{\ell+m}(Y + y_i)$. Let $g_0, h_0$ be generators of $\mathbb{G}_1$ and $\mathbb{G}_2$ and pick $k, \gamma, \alpha, \beta \xleftarrow{R} \mathbb{Z}_p$. The $(\ell, m, t)$-aMSE-DDH assumption states that given

$$g_0, g_0^{\gamma}, \ldots, g_0^{\gamma^{\ell+t-2}}, \quad g_0^{k\gamma f(\gamma)}, \quad h_0, h_0^{\gamma}, \ldots, h_0^{\gamma^{m-2}}, \quad h_0^{kg(\gamma)},$$
$$g_0^{\beta\gamma}, \ldots, g_0^{\beta\gamma^{\ell+t-2}}, \quad h_0^{\beta}, h_0^{\beta\gamma}, \ldots, h_0^{\beta\gamma^{m-1}},$$
$$g_0^{\alpha}, g_0^{\alpha\gamma}, \ldots, g_0^{\alpha\gamma^{\ell+t}}, \quad h_0^{\alpha}, h_0^{\alpha\gamma}, \ldots, h_0^{\alpha\gamma^{2(m-t)+3}},$$

and $T \in \mathbb{G}_T$, it is hard to determine whether $T = e(g_0, h_0)^{kf(\gamma)}$ or $T \in_R \mathbb{G}_T$.

We observe that the first line of the input is quite similar to the input of the GDDHE assumption [26] (cf. Sect. 3.1). We can transpose the discussion in Sect. 3.1 to the aMSE-DDH assumption. As we have shown, the gap between the uber assumption [23] and the aMSE-DDH assumption is due to the structures of polynomials in the exponents of $h_0$ and the entry $g_0^{k\gamma f(\gamma)}$ which shares $kf(\gamma)$ with the challenge. We therefore conclude that the Déjà Q framework [23] does not subsume the $(\ell, m, t)$-aMSE-DDH assumption.

In this section as well, we are not going to start from the aMSE-DDH assumption. Instead, we will try to adapt Herranz *et al.*'s prime-order construction [37] into composite-order groups and analyse its selective security directly. Our fuzzy IBE scheme preserves the advantages of Herranz *et al.*'s [37] such as constant-size ciphertexts and can now be proved secure under static assumptions.

### 4.1 Construction

Before presenting the construction, we describe algorithm Aggregate of [4,27].

**Aggregate Algorithm.** The Aggregate algorithm of [27] was given for elements in $\mathbb{G}_T$, but it carries over to any prime order group [4]. Our construction requires it to work in composite order groups. Let a cyclic group $\mathbb{G}$ of composite order

[4] The assumption is originally given in symmetric groups. In order to work with the Déjà Q framework, one must transform it into asymmetric groups (using Abe *et al.*'s method [3] as suggested in [23]) which depends on the scheme and the reduction.

$N$. Given a set of pairs $\{u^{\frac{1}{\alpha+x_i}}, x_i\}_{i=1}^n$, where $u \in \mathbb{G}$ and $\alpha \in \mathbb{Z}_N$ are unknown and $x_1, \ldots, x_n \in \mathbb{Z}_N$ are pairwise distinct elements such that

$$\gcd(x_i - x_j, N) = 1 \quad \text{for all } i \neq j, \tag{1}$$

the algorithm computes the value $\mathsf{Aggregate}(\{u^{\frac{1}{\alpha+x_i}}, x_i\}_{i=1}^n) = u^{\frac{1}{\prod_{i=1}^n (\alpha+x_i)}}$ using $O(n^2)$ exponentiations. (See the full version [33] for details.) It is unlikely to encounter a pair $(x_i, x_j)$ violating restriction (1) since it exposes a non-trivial factorisation of $N$ and violates the decisional subgroup assumption.

**Our Fuzzy IBE Construction.** In the description hereunder, we denote by $n$ an upper bound on the number $\ell$ of attributes per identity. The construction goes as follows.

$\mathsf{Setup}(1^\lambda, 1^n)$**:** Choose $\rho \in \mathsf{poly}(\lambda)$ and define $\mathcal{M} = \{0,1\}^\rho$. Generate a composite-order pairing ensemble $(\mathcal{G} = (p_1, p_2, p_3, \mathbb{G}, \mathbb{G}_T, e)) \longleftarrow \mathsf{GroupGen}(\rho + 2\lambda, 3)$ and set $N = p_1 p_2 p_3$. Then, arbitrarily select $n-1$ distinct dummy identities $d_1, \ldots, d_{n-1} \in \mathbb{Z}_N$. Define the set $\mathcal{I} = \mathbb{Z}_N \setminus \{d_1, \ldots, d_{n-1}\}$. Pick $g, u_0 \xleftarrow{R} \mathbb{G}_{p_1}^\times$ and $g_3 \xleftarrow{R} \mathbb{G}_{p_3}^\times$ and choose $\alpha, \gamma \xleftarrow{R} \mathbb{Z}_N$. Let $\mathsf{H} : \mathbb{G}_T \to \{0,1\}^\rho$ be a universal hash function. Define $\mathsf{MSK} = (u_0, \alpha, \gamma, g_3)$ while the public parameters consist of

$$\mathsf{PP} = \big(\mathcal{G}_{\text{pub}},\ g,\ g^\gamma,\ \big(G_i = g^{\alpha^i}\big)_{i=1}^{2n-1},\ e(g,u_0)^\gamma,\ (d_i)_{i=1}^{n-1},\ \mathsf{H}\big).$$

$\mathsf{KeyGen}(\mathsf{MSK}, S = \{\mathsf{id}_1, \ldots, \mathsf{id}_\ell\})$**:** Pick $u \xleftarrow{R} \mathbb{G}_{p_1}, X_{3,1}, \ldots, X_{3,\ell}, X'_{3,1}, \ldots, X'_{3,n-1}, X_{3,0} \xleftarrow{R} \mathbb{G}_{p_3}$ (using generator $g_3$) and output the secret key

$$\mathsf{SK}_S = \big(\big(K_i = u^{\frac{\gamma}{\alpha+\mathsf{id}_i}} \cdot X_{3,i}\big)_{i=1}^{\ell},\quad \big(K'_i = u^{\alpha^i} \cdot X'_{3,i}\big)_{i=1}^{n-1},\quad K_0 = u \cdot u_0 \cdot X_{3,0}\big).$$

$\mathsf{Encrypt}(\mathsf{PP}, S = \{\mathsf{id}_1, \ldots, \mathsf{id}_\ell\}, \tau \leq \ell, M)$**:** To encrypt $M \in \{0,1\}^\rho$ for the set $S$ with threshold $\tau$, compute coefficients $\{c_j\}_{j \in [0, n+\tau-1]}$ for the polynomial

$$p_{S,\tau}(x) = \prod_{i=1}^{\ell}(x + \mathsf{id}_i) \cdot \prod_{i=1}^{n+\tau-1-\ell}(x + d_i) = \sum_{i=0}^{n+\tau-1} c_i x^i \in \mathbb{Z}_N[x].$$

Choose $s \xleftarrow{R} \mathbb{Z}_N$ and output the ciphertext $\mathsf{CT}_{S,\tau}$ consisting of

$$C_0 = M \oplus \mathsf{H}(e(g,u_0)^{s\gamma}), \quad C_1 = g^{s\gamma}, \quad C_2 = \big(g^{c_0} \cdot \prod_{i=1}^{n+\tau-1} G_i^{c_i}\big)^s = g^{s \cdot p_{S,\tau}(\alpha)}.$$

$\mathsf{Decrypt}(\mathsf{PP}, S, \tau, \mathsf{CT}, S', \mathsf{SK}_{S'})$**:** If $|S \cap S'| < \tau$, return $\perp$. Otherwise, we can find a set $\bar{S} \subseteq \mathcal{I}$ satisfying $\bar{S} \subseteq S \cap S'$ and $|\bar{S}| = \tau$. Note that the choice of $\bar{S}$ is arbitrary. By invoking algorithm $\mathsf{Aggregate}$, we can compute

$$K_{\mathsf{Agg}} = u^{\frac{\gamma}{\prod_{\mathsf{id} \in \bar{S}}(\alpha+\mathsf{id})}} \cdot X_{3,\mathsf{Agg}}$$

for some $X_{3,\mathsf{Agg}} \in \mathbb{G}_{p_3}$. Let

$$op_{S,\bar{S},\tau}(x) = p_{S,\tau}(x) / \textstyle\prod_{\mathsf{id} \in \bar{S}}(x + \mathsf{id}) = \sum_{i=0}^{n-1} z_i x^i$$

where $z_0 = \prod_{\mathsf{id} \in S \setminus \bar{S}} \mathsf{id} \cdot \prod_{i=1}^{n+\tau-1-|S|} d_i$. We can compute

$$A_1 = e(C_1, \prod_{i=1}^{n-1}(K_i')^{z_i}) = e(g^{s\gamma}, u^{p_{S,\bar{S},\tau}(\alpha)-z_0}) = e(g,u)^{s\gamma(p_{S,\bar{S},\tau}(\alpha)-z_0)},$$
$$A_2 = e(C_2, K_{\mathsf{Agg}}) = e(g^{s \cdot p_{S,\tau}(\alpha)}, u^{\frac{\gamma}{\prod_{\mathsf{id}\in\bar{S}}(\alpha+\mathsf{id})}} \cdot X_{3,\mathsf{Agg}}) = e(g,u)^{s\gamma p_{S,\bar{S},\tau}(\alpha)},$$
$$A_3 = e(C_1, K_0) = e(g^{s\gamma}, u \cdot u_0 \cdot X_{3,0}) = e(g,u)^{s\gamma} \cdot e(g,u_0)^{s\gamma},$$

and recover the message as $M = C_0 \oplus \mathsf{H}\big(A_3/(A_2/A_1)^{1/z_0}\big)$.

The scheme is easily seen to be correct. We note that Decrypt can be optimized to consume only 2 pairing operations by recovering $e(g,u)^{s\gamma} = e(C_1, K_0 \cdot (\prod_{i=1}^{n-1}(K_i')^{z_i})^{1/z_0})/e(C_2, K_{\mathsf{Agg}}^{1/z_0})$.

### 4.2 Proof of Security

We give the following theorem and refer to the full version [33] for the proof.

**Theorem 2.** *For any adversary $\mathscr{A}$ attacking $\mathcal{FIBE}$ in the* sid-cpa *model making at most $q$ key extraction queries, there exist algorithms $\mathscr{B}_1, \mathscr{B}_2$ such that*

$$\mathsf{Adv}^{\mathscr{A}}_{\mathcal{FIBE},\mathsf{sid\text{-}cpa}}(\lambda) \leq 2 \cdot \mathsf{Adv}^{\mathscr{B}_1}_{\mathcal{G},\mathrm{DS1}}(\lambda) + (\ell+n+2) \cdot \mathsf{Adv}^{\mathscr{B}_2}_{\mathcal{G},\mathrm{DS2}}(\lambda) + \frac{q \cdot (\ell+2n)^2}{p_2} + \frac{1}{p_2} + \frac{1}{2^\lambda}.$$

*where $\ell$ is maximum size of attribute sets.*

**Acknowledgements.** We want to thank all anonymous reviewers for invaluable comments. This work was funded in part by the "Programme Avenir Lyon Saint-Etienne de l'Université de Lyon" in the framework of the programme "Investissements d'Avenir" (ANR-11-IDEX-0007) and by the French ANR ALAMBIC project (ANR-16-CE39-0006). Part of this work was done when the last author was at Laboratoire LIP, ENS de Lyon, France and Indian Institute of Technology Bhubaneswar, India.

## References

1. Abdalla, M., et al.: Searchable encryption revisited: consistency properties, relation to anonymous IBE, and extensions. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 205–222. Springer, Heidelberg (2005). https://doi.org/10.1007/11535218_13
2. Abdalla, M., Kiltz, E., Neven, G.: Generalized key delegation for hierarchical identity-based encryption. In: Biskup, J., López, J. (eds.) ESORICS 2007. LNCS, vol. 4734, pp. 139–154. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74835-9_10
3. Abe, M., Groth, J., Ohkubo, M., Tango, T.: Converting cryptographic schemes from symmetric to asymmetric bilinear groups. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014. LNCS, vol. 8616, pp. 241–260. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-44371-2_14
4. Attrapadung, N., Herranz, J., Laguillaumie, F., Libert, B., de Panafieu, E., Ràfols, C.: Attribute-based encryption schemes with constant-size ciphertexts. Theor. Comput. Sci. **422**, 15–38 (2012)

5. Attrapadung, N., Libert, B.: Functional encryption for inner product: achieving constant-size ciphertexts with adaptive security or support for negation. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 384–402. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13013-7_23
6. Attrapadung, N., Libert, B., de Panafieu, E.: Expressive key-policy attribute-based encryption with constant-size ciphertexts. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 90–108. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19379-8_6
7. Attrapadung, N.: Dual system encryption via doubly selective security: framework, fully secure functional encryption for regular languages, and more. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 557–577. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55220-5_31
8. Bellare, M., Rogaway, P.: Random oracles are practical: a paradigm for designing efficient protocols. In: 1st ACM Conference on Computer and Communications Security (1993)
9. Boneh, D., Boyen, X., Goh, E.-J.: Hierarchical identity based encryption with constant size ciphertext. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 440–456. Springer, Heidelberg (2005). https://doi.org/10.1007/11426639_26
10. Boneh, D., Di Crescenzo, G., Ostrovsky, R., Persiano, G.: Public key encryption with keyword search. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 506–522. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24676-3_30
11. Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. SIAM J. Comput. **32**(3), 586–615 (2003). Earlier version in CRYPTO 2001. LNCS, vol. 2139, pp. 213–229 (2001)
12. Boneh, D., et al.: Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 533–556. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55220-5_30
13. 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
14. Boneh, D., Hamburg, M.: Generalized identity based and broadcast encryption schemes. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 455–470. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-89255-7_28
15. 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
16. Boneh, D., Waters, B., Zhandry, M.: Low overhead broadcast encryption from multilinear maps. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014. LNCS, vol. 8616, pp. 206–223. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-44371-2_12
17. Boyen, X., Waters, B.: Anonymous hierarchical identity-based encryption (without random oracles). In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 290–307. Springer, Heidelberg (2006). https://doi.org/10.1007/11818175_17
18. Canetti, R., Halevi, S., Katz, J.: A forward-secure public-key encryption scheme. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 255–271. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-39200-9_16

19. Chen, J., Gong, J., Weng, J.: Tightly secure IBE under constant-size master public key. In: Fehr, S. (ed.) PKC 2017. LNCS, vol. 10174, pp. 207–231. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-662-54365-8_9
20. Chen, J., Libert, B., Ramanna, S.C.: Non-zero inner product encryption with short ciphertexts and private keys. In: Zikas, V., De Prisco, R. (eds.) SCN 2016. LNCS, vol. 9841, pp. 23–41. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-44618-9_2
21. Chen, J., Wee, H.: Semi-adaptive attribute-based encryption and improved delegation for boolean formula. In: Abdalla, M., De Prisco, R. (eds.) SCN 2014. LNCS, vol. 8642, pp. 277–297. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-10879-7_16
22. Chase, M., Meiklejohn, S.: Déjà Q: using dual systems to revisit $q$-type assumptions. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 622–639. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55220-5_34
23. Chase, M., Maller, M., Meiklejohn, S.: Déjà Q all over again: tighter and broader reductions of $q$-type assumptions. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10032, pp. 655–681. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53890-6_22
24. Cheon, J.H.: Security analysis of the strong diffie-hellman problem. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 1–11. Springer, Heidelberg (2006). https://doi.org/10.1007/11761679_1
25. Cheon, J.H., Han, K., Lee, C., Ryu, H., Stehlé, D.: Cryptanalysis of the multilinear map over the integers. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 3–12. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46800-5_1
26. Delerablée, C.: Identity-based broadcast encryption with constant size ciphertexts and private keys. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 200–215. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-76900-2_12
27. Delerablée, C., Pointcheval, D.: Dynamic threshold public-key encryption. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 317–334. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85174-5_18
28. Derler, D., Jager, T., Slamanig, D., Striecks, C.: Bloom filter encryption and applications to efficient forward-secret 0-RTT key exchange. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018. LNCS, vol. 10822, pp. 425–455. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-78372-7_14
29. 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
30. Freeman, D.M.: Converting pairing-based cryptosystems from composite-order groups to prime-order groups. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 44–61. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_3
31. Gay, R., Kerenidis, I., Wee, H.: Communication complexity of conditional disclosure of secrets and attribute-based encryption. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9216, pp. 485–502. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48000-7_24
32. Garg, S., Gentry, C., Halevi, S., Raykova, M., Sahai, A., Waters, B.: Candidate indistinguishability obfuscation and functional encryption for all circuits. In: FOCS 2013 (2013)

33. Gong, J., Libert, B., Ramanna, S.C.: Compact IBBE and Fuzzy IBE from Simple Assumptions. https://hal.inria.fr/hal-01686690/
34. 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
35. Gorbunov, S., Vaikuntanathan, V., Wee, H.: Attribute-based encryption for circuits from LWE. In: STOC 2013 (2013)
36. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: ACM CCS 2006 (2006)
37. Herranz, J., Laguillaumie, F., Ràfols, C.: Constant size ciphertexts in threshold attribute-based encryption. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 19–34. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13013-7_2
38. Hohenberger, S., Waters, B.: Attribute-based encryption with fast decryption. In: Kurosawa, K., Hanaoka, G. (eds.) PKC 2013. LNCS, vol. 7778, pp. 162–179. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-36362-7_11
39. Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Smart, N. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 146–162. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-78967-3_9
40. Lewko, A., Sahai, A., Waters, B.: Revocation systems with very small private keys. In: 2010 IEEE Symposium on Security and Privacy (2010)
41. 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
42. Lewko, A., Waters, B.: New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 455–479. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-11799-2_27
43. Naor, M., Naor, D., 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
44. Naor, M., Pinkas, B.: Efficient trace and revoke schemes. In: Frankel, Y. (ed.) FC 2000. LNCS, vol. 1962, pp. 1–20. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45472-1_1
45. Nguyen, L.: Accumulators from bilinear pairings and applications. In: Menezes, A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 275–292. Springer, Heidelberg (2005). https://doi.org/10.1007/978-3-540-30574-3_19
46. 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
47. Okamoto, T., Takashima, K.: Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption. In: Lin, D., Tsudik, G., Wang, X. (eds.) CANS 2011. LNCS, vol. 7092, pp. 138–159. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25513-7_11
48. Okamoto, T., Takashima, K.: Fully secure unbounded inner-product and attribute-based encryption. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 349–366. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34961-4_22

49. Okamoto, T., Takashima, K.: Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption. Des. Codes Crypt. **77**(2–3), 725–771 (2015)
50. Ostrovsky, R., Sahai, A., Waters, B.: Attribute-based encryption with non-monotonic access structures. In: ACM CCS 2007 (2007)
51. Rouselakis, Y., Waters, B.: Practical constructions and new proof methods for large universe attribute-based encryption. In: ACM CCCS 2013 (2013)
52. Sakai, R., Furukawa, J.: Identity-based broadcast encryption. In: Cryptology ePrint Archive: Report 2007/217 (2007). http://eprint.iacr.org/2007/217
53. Sakai, R., Kasahara, M.: ID-based cryptosystems with pairing on elliptic curve. In: Cryptology ePrint Archive: Report 2003/054 (2003). http://eprint.iacr.org/2003/054
54. 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
55. 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
56. Takashima, K.: Expressive attribute-based encryption with constant-size ciphertexts from the decisional linear assumption. In: Abdalla, M., De Prisco, R. (eds.) SCN 2014. LNCS, vol. 8642, pp. 298–317. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-10879-7_17
57. Takashima, K.: New proof techniques for DLIN-based adaptively secure attribute-based encryption. In: Pieprzyk, J., Suriadi, S. (eds.) ACISP 2017. LNCS, vol. 10342, pp. 85–105. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-60055-0_5
58. Waters, B.: Efficient identity-based encryption without random oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005). https://doi.org/10.1007/11426639_7
59. Waters, B.: Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 619–636. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03356-8_36
60. Waters, B.: Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 53–70. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19379-8_4
61. Waters, B.: Functional encryption for regular languages. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 218–235. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32009-5_14
62. 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