A Profitable Sub-Prime Loan: Obtaining the Advantages of Composite-Order in Prime-Order Bilinear Groups

Allison Lewko
Microsoft Research New England
allew@microsoft.com

Sarah Meiklejohn
UC San Diego
smeiklej@cs.ucsd.edu

Abstract

Composite-order bilinear groups provide many structural features that have proved useful for both constructing cryptographic primitives and as a technique in security reductions. Despite these convenient features, however, composite-order bilinear groups are less desirable than prime-order bilinear groups for reasons of efficiency. A recent line of work has therefore focused on translating these structural features from the composite-order to the prime-order setting; much of this work focused on two such features, projecting and canceling, in isolation, but a recent result due to Seo and Cheon showed that both features can be obtained simultaneously in the prime-order setting.

In this paper, we reinterpret the construction of Seo and Cheon in the context of dual pairing vector spaces, a tool previously used to simulate other desirable features of composite-order groups in the prime-order setting. In this way, we are able to obtain a unified framework that simulates all of the known composite-order features in the prime-order setting. We demonstrate the strength of this framework by showing that the addition of even a weak form of projecting on top of the pre-existing uses of dual pairing vector spaces can be leveraged to "boost" a fully IND-CPA secure identity-based encryption scheme to one that is fully IND-CCA1 secure.

1 Introduction

Since their introduction in 2005 by Boneh, Goh, and Nissim [7], composite-order bilinear groups have been used to construct a diverse set of advanced cryptographic primitives, including (hierarchical) identity-based encryption [20, 22], group signatures [9, 10], and functional and attribute-based encryption [17, 21, 19]. The main assumptions used to prove the security of such schemes are variants of the *subgroup decision* assumption, which (in the simplest case) states that, for a bilinear group G of order $N = pq$, without an element of order q it should be hard to distinguish a random element of G from a random element of order p. Such assumptions crucially rely on the hardness of factoring N.

Beyond this basic assumption and its close variants, many of these schemes have exploited additional structural properties that come with using composite-order bilinear groups. Two such properties, *projecting* and *canceling*, were formally identified by Freeman [13]; projecting requires (roughly) that there exists a trapdoor projection map from G into its p-order subgroup (and a related map in the target group G_T), and canceling requires that elements in the p-order and q-order subgroups cancel each other out (i.e., yield the identity when paired). Additionally, Lewko [18] identified another property, *parameter hiding*, that requires (again, roughly) that elements in the p-order subgroup reveal nothing about seemingly correlated elements in the q-order subgroup.

While therefore quite attractive and rich from a structural standpoint, the use of composite-order bilinear groups comes with a number of drawbacks, both in terms of efficiency and security. Until a recent construction of Boneh, Rubin, and Silverberg [8], all known composite-order bilinear groups were on supersingular, or Type-1 [14], curves. Even in the prime-order setting, supersingular curves are already less efficient than their ordinary counterparts: speed records for the former [1, 28] are approximately six times slower than speed records for the latter [2]. In the composite-order setting, it is furthermore necessary to increase the size of the modulus by at least a factor of 10 (from 160 to at least 1024 bits) in order to make the assumption that N is hard to factor plausible. Operations performed in composite-order bilinear groups are therefore significantly slower; for example, Guillevic [15] recently observed that computing a pairing was 254 times slower. (This slowdown also extends to the non-supersingular construction of Boneh et al., and indeed to any composite-order bilinear group.) Furthermore, from a security standpoint, a recent result due to Hayashi et al. [16] demonstrates that in a common type of supersingular curve, namely one with embedding degree $k = 6$, it is possible to efficiently compute discrete logarithms; this result demonstrates that working in supersingular curves is perhaps more "dangerous" than working in their non-supersingular counterparts.

One natural question to ask is: to what extent it is possible to obtain the structural advantages of composite-order bilinear groups without the disadvantages? Although the structural properties described above might seem specific to composite-order groups, both Freeman and Lewko are in fact able to express them rather abstractly and then describe how to construct prime-order bilinear groups in which each of these individual properties are met; they also show how to translate the subgroup decision assumption into a generalized version, that in prime-order groups is implied by either Decision Linear [6] or Symmetric External Diffie Hellman (SXDH) [3].

In contrast, Meiklejohn, Shacham, and Freeman [24] showed that it was impossible to achieve projecting and canceling simultaneously under a "natural" usage of Decision Linear; as a motivation, they presented a blind signature scheme that seemingly relied upon both projecting and canceling for its proof of security. Recently, Seo and Cheon [30] showed that it was actually possible to achieve both projecting and canceling simultaneously in prime-order groups, and Seo [29] explored both possibility and impossibility results for projecting. To derive hardness of subgroup decision in their setting, however, Seo and Cheon rely on a non-standard assumption and show that this implies the hardness of subgroup decision only in a very limited case. They also provide a prime-order version of the Meiklejohn et al. blind signature that is somewhat divorced from their setting: rather than prove its security directly using projecting and canceling, they instead alter the blind signature, introduce a new property called *translating*, and then show that the modified blind signature is secure not in the projecting and canceling setting, but rather in a separate projecting and translating setting.

Our contributions. In this paper, we present in Section 3 an abstract presentation of the projecting and canceling pairing due to Seo and Cheon [30]; in the process, we eliminate their reliance on a non-standard assumption for some instances of subgroup decision. Our presentation is based on dual pairing vector spaces [25, 26], and it can be parameterized to yield projection properties of varying strength. This perspective yields several advantages. First, all the power of dual pairing vector spaces is embedded inside this construction and can thus be exploited as in prior works. Second, we observe that even weak projection properties are useful, and when these suffice, the hardness of subgroup decision problems is implied by SXDH. As the projection properties are strengthened, reducing to SXDH seems to become difficult, and we leave it as an interesting open problem to obtain a larger class of subgroup decision variants from just the SXDH assumption in the presence of strong projection properties. If one is willing to rely on non-standard (though still static) assumptions that can be justified in the generic group model, then we suspect that all subgroup decision variants can be obtained simultaneously with the strongest combination of properties.

Next, in Section 4, we present an IND-CCA1-secure identity-based encryption (IBE) scheme that uses canceling, parameter hiding, and weak projecting properties in its proof of security. Although efficient constructions of IND-CCA2-secure IBE schemes have been previously obtained by combining IND-CPA-secure HIBE schemes with signatures [11], we nevertheless view our IBE construction as a demonstration of the applicability of our unified framework, since it leverages the combined power of dual pairing vector spaces and a form of projecting. Furthermore, our new construction does not aim to amplify security by adding new primitives; instead, it explores the existing security of the IND-CPA-secure IBE due to Boneh and Boyen [5] (which cannot be IND-CCA2 secure, as it has re-randomizable ciphertexts), and observes that, by modifying the scheme in a rather organic way and exploiting the (weak) projecting and canceling properties of the setting, we can prove IND-CCA1 security directly. In addition, our techniques demonstrate that the same subgroup structures that were used by Lewko and Waters [20] to "boost" from selective to full IND-CPA security can be further applied to "boost" all the way to full IND-CCA1-security. We therefore view our scheme as a proof of concept for the usefulness of obtaining projecting and canceling simultaneously in the prime-order setting, and believe that the usefulness of our framework extends well beyond this IBE application. We intend our work to facilitate future applications of these combined properties.

Our techniques To obtain a more user-friendly interpretation of the projecting and canceling pairing construction over prime-order groups, we begin by observing that it is essentially a concatenation of dual pairing vector spaces (DPVS). Dual pairing vector spaces were first used in prime order bilinear groups by Okamoto and Takashima [25, 26] and have since been employed in many works, in particular to instantiate dual system encryption proof techniques (as introduced by Waters [31]) in the prime-order setting [19, 27, 18]. These previous uses of DPVS typically relied on the canceling property, variants of subgroup decision problems, and certain parameter hiding properties that are present by design in DPVS. One particularly nice feature of DPVS constructions is that a large family of useful subgroup decision variants can be proven to follow from standard assumptions like SXDH for asymmetric groups and DLIN for symmetric groups; viewing the construction of a projecting and canceling pairing as a natural extension of DPVS therefore has the twin benefits that it provides a clear guide on how to derive certain subgroup decision variants from standard assumptions, and that it comes with all the built-in tools that DPVS has to offer.

In particular, DPVS have already been used by Lewko [18] to build a fully IND-CPA-secure identity-based encryption scheme that mirrors the structure of the selectively-secure Boneh-Boyen scheme; this was accomplished by translating a fully secure composite-order variant [20]. (An asymmetric variant of this scheme was also given by Chen et al. [12].) Now that we have added in projection, we can use it to boost this scheme to full IND-CCA1 security; again, as the core IBE scheme is re-randomizable, we cannot hope to achieve IND-CCA2 security without departing from the core structure of the scheme. Hence, we view this as an exploration of the kinds of security properties that can be proven solely from the minimalistic spirit of the Boneh-Boyen scheme.

Our technique for proving IND-CCA1 security extends from the observation due to Lewko and Waters [23] that dual system encryption proofs can be interpreted as a reduction from a full security game to a weak game in which the attacker does not have access to the public parameters. Using this technique, we first define such a weak game for IND-CCA1 security, and then prove that our IBE construction satisfies it; this is an easier task than proving full IND-CCA1 security directly, as in particular the absence of public parameters makes it difficult for the attacker to produce meaningful decryption queries. Next, leveraging the addition of projection, we reduce the full IND-CCA1 security to this weaker notion by first expanding the system to have extra components in a space that is not reflected in the public parameters, and then projecting to play the weak game in that space. We formulate our IBE scheme and proof in a unified framework that can be instantiated, as we will see in Sections 4 and 5, over prime-order or composite-order bilinear groups (relying on SXDH or generalized subgroup decision [4] respectively).

2 Definitions and Notation

In this section, we define bilinear groups and the three functional properties we would like them to satisfy: projecting, canceling, and parameter hiding. For the first two, we use the definitions of Freeman [13] (albeit in a somewhat modified form); for parameter hiding, on the other hand, we come up with a new formal framework. In addition to these functional properties, we consider the notion of subgroup decision in bilinear groups, in which a random element of a subgroup should be indistinguishable from a random element of the full group. The variant we define, called generalized correlated subgroup decision, is very general: in addition to seeing random elements of subgroups, we allow an attacker to see elements *correlated* across subgroups (e.g., elements of different subgroups with correlated randomness), and require that it is still difficult for him to distinguish between correlated elements of different subgroups. We then see in Sections 3 and 5 that many specific instances of this general notion are implied by more standard notions of subgroup decision in both prime-order and composite-order groups.

2.1 Bilinear groups

In what follows, we refer to a *bilinear group* as a tuple $\mathbb{G} = (N, G, H, G_T, e, \mu)$, where N is either prime or composite, $|G| = |H| = kN$ and $|G_T| = \ell N$ for some $k, \ell \in \mathbb{N}$, and $e : G \times H \to G_T$ is a bilinear map; i.e., e is an efficient map that satisfies both *bilinearity* ($e(x^a, y^b) = e(x, y)^{ab}$ for all $x \in G$, $y \in H$, $a, b \in \mathbb{Z}/N\mathbb{Z}$) and *non-degeneracy* ($e(x, y) = 1$ only if $x = 1$ or $y = 1$). In some bilinear groups, we may additionally include generators g and h of G and H respectively (if G and H are cyclic), information about meaningful subgroups of G and H, or some auxiliary information μ that allows for efficient membership testing in G and H (and possibly more). In what follows, we refer to the algorithm that is used to generate such groups $\mathbb{G}$ as $\mathsf{BilinearGen}$, and note that, beyond the security parameter, $\mathsf{BilinearGen}$ takes in an additional parameter n that specifies the number of desired subgroups; i.e., for $(N, G, H, G_T, e, \mu) \xleftarrow{\$} \mathsf{BilinearGen}(1^k, n)$, we have $G = \oplus_{i=1}^n G_i$ and $H = \oplus_{i=1}^n H_i$ (where typically G_i and H_i are cyclic).

In terms of functional properties of bilinear groups, we first define both *projecting* and *canceling*; our definitions are modified versions of the ones originally given by Freeman [13]. We give three flavors of projecting. The first, *weak projecting*, considers projecting into a single subgroup of the source group, without requiring a corresponding map in the target group. The second, which we call simply *projecting*, most closely matches the definition given by Freeman, and considers projecting into a single subgroup in both the source and target groups. Lastly, we define *full* projecting, which considers projecting into every subgroup individually. As we will see in Section 3, we can satisfy all of these flavors by tweaking appropriate parameters in our prime-order construction.

Definition 2.1 (Weak projecting)**.** *A bilinear group $\mathbb{G} = (N, G, H, G_T, e, \mu)$ is* weakly projecting *if there exist decompositions $G = G_1 \oplus G_2$ and $H = H_1 \oplus H_2$, and projection maps π_G and π_H such that $\pi_G(x_1) = x_1$ for all $x_1 \in G_1$ and $\pi_G(x_2) = 1$ for all $x_2 \in G_2$, and similarly $\pi_H(y_1) = y_1$ for all $y_1 \in H_1$ and $\pi_H(y_2) = 1$ for all $y_2 \in H_2$.*

Definition 2.2 (Projecting)**.** *A bilinear group $\mathbb{G} = (N, G, H, G_T, e, \mu)$ is* projecting *if there exist subgroups $G' \subset G$, $H' \subset H$, and $G'_T \subset G_T$ such that there exist non-trivial maps $\pi_G : G \to G'$, $\pi_H : H \to H'$, and $\pi_T : G_T \to G'_T$ such that $\pi_T(e(x, y)) = e(\pi_G(x), \pi_H(y))$ for all $x \in G$, $y \in H$.*

Definition 2.3 (Full projecting)**.** *A bilinear group $\mathbb{G} = (N, G, H, G_T, e, \mu)$ is* fully projecting *if there exists some $n \in \mathbb{N}$ and decompositions $G = \oplus_{i=1}^n G_i$, $H = \oplus_{i=1}^n H_i$, and $G_T = \oplus_{i=1}^n G_{T,i}$, and non-trivial maps $\pi_{Gi} : G \to G_i$, $\pi_{Hi} : H \to H_i$, and $\pi_{Ti} : G_T \to G_{T,i}$ for all i such that $\pi_{Ti}(e(x, y)) = e(\pi_{Gi}(x), \pi_{Hi}(y))$ for all $x \in G$, $y \in H$.*

Definition 2.4 (Canceling)**.** *A bilinear group $\mathbb{G} = (N, G, H, G_T, e, \mu)$ is* canceling *if there exists some $n \in \mathbb{N}$ and decompositions $G = \oplus_{i=1}^{n} G_i$ and $H = \oplus_{i=1}^{n} H_i$ such that $e(x_i, y_j) = 1$ for all $x_i \in G_i$, $y_j \in H_j$, $i \neq j$.*

2.2 Parameter hiding

Beyond projecting and canceling, we aim to define *parameter hiding*. As mentioned in the introduction, this property roughly says that elements in one subgroup should not reveal anything about related elements in other subgroups, and was previously used, without a formal definition, by Lewko [18].

The main difficulty in providing a formal definition for parameter hiding is that it is not as self-contained a feature as projecting and canceling; elements within subgroups may be related to elements in other subgroups in a myriad of ways, and their relation to one another may depend both on the form of the element (which can essentially be any function on the exponents; e.g., $g_1^{ax} g_2^{bx^2} g_3^{cx^3}$ or $g_1^{ax-by+cz} g_2^{ay-bx+2cz}$) and on the subgroups. We therefore do not try to consider all types of correlations, but instead focus on one simple type, defined as follows:

Definition 2.5. *For a bilinear group $\mathbb{G} = (N, G = \oplus_{i=1}^{n} G_i, H = \oplus_{i=1}^{n} H_i, G_T, e, \{g_i\}_{i=1}^{n}, \{h_i\}_{i=1}^{n})$, an element $x \in \mathbb{Z}/N\mathbb{Z}$, and indices $1 \leq i_1, i_2 \leq n$, an x-*correlated sample *from the subgroup $G_{i_1} \oplus G_{i_2}$ is an element of the form $g_{i_1}^{\alpha} \cdot g_{i_2}^{\alpha x}$ for $\alpha \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$.*

We also consider correlated samples in H, but for convenience we will define a y-correlated sample from the subgroup $H_{i_1} \oplus H_{i_2}$ to be an element of the form $h_{i_1}^{\beta y} \cdot h_{i_2}^{\beta}$ for $\beta \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$. (Note that the y is now on the first subgroup instead of the second.)

Although we choose this type of correlation mainly for ease of exposition (and because we encounter it in Section 4), our discussion below could be adjusted to accommodate more general types of correlation, and this would remain compatible with our prime-order construction in Section 3.

Intuitively then, parameter hiding says that, under certain restrictions about which subgroup elements one is allowed access to, the distributions over x-correlated samples and random samples should in fact be the same, even when x is known. (We will need some restrictions because there may be testable relationships between the images of various generators in the target group. We will give a concrete example below.) To consider which kinds of distributions we can use; i.e., what additional information we might give out besides the samples, we consider distributions $\mathcal{D}$ parameterized by multisets S_G, S_H, X, and Y, and a set C; intuitively, the sets S_G and S_H tell us which elements to include in the distribution, the sets X and Y tell us which correlated samples to include (e.g., x_i-correlated samples for all $x_i \in X$), and the set C tells us which correlated samples to change to random. Formally then, we have $S_G = \{s_1, \ldots, s_{k_1}; t_1, \ldots, t_{k_2}; c_1, \ldots, c_{k_3}\}$ and $S_H = \{s'_1, \ldots, s'_{\ell_1}; t'_1, \ldots, t'_{\ell_2}; c'_1, \ldots, c'_{\ell_3}\}$, where S_G indicates elements to include in the distribution as follows:

- For all $s_i \in S_G$, include g_{s_i} in $\mathcal{D}$.
- For all $t_i = (t_{1,i}, \ldots, t_{m,i}) \in S_G$, include a random sample from $G_{t_{1,i}} \oplus \ldots \oplus G_{t_{m,i}}$ in $\mathcal{D}$. (This is why we use multisets, as we may want multiple random samples from the same subgroups.)
- For all $c_i = (c_{1,i}, c_{2,i}) \in S_G$, include an x_i-correlated sample from $G_{c_{1,i}} \oplus G_{c_{2,i}}$ in $\mathcal{D}$; i.e., a sample of the form $g_{c_{1,i}}^{a} \cdot g_{c_{2,i}}^{a x_i}$ for $a \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$.

The set S_H is defined analogously for the group H, with respect to the set Y. To now consider changing correlated samples to random, we use $C \subseteq \{c_1, \ldots, c_{k_3}; c'_1, \ldots, c'_{\ell_3}\}$ to indicate which correlated samples to change; for $C = \emptyset$, parameter hiding trivially holds (as none of the samples are changed).

Given all these sets, we now place our restrictions on them by requiring that they are *well-behaved* in the following two ways: (1) for any changed x-correlated sample in some subgroup, do not reveal the corresponding generators on either side of the pairing, and (2) do not change correlated samples for the same value x on opposite sides of the pairing. Formally, we express these requirements as

- Don't include generators for switched samples. For all $(c_{1,i}, c_{2,i}) \in C$, $s_j \in S_G$, and $s'_\ell \in S_H$, $s_j \neq c_{1,i}, c_{2,i}$ and $s'_\ell \neq c_{1,i}, c_{2,i}$; analogously, for all $(c'_{1,i}, c'_{2,i}) \in C$, $s_j \in S_G$, and $s'_\ell \in S_H$, $s_j \neq c'_{1,i}, c'_{2,i}$ and $s'_\ell \neq c'_{1,i}, c'_{2,i}$.
- Don't switch x-correlated samples in G and H. For all $c_i, c'_j \in C$, $x_i \neq y_j$.

To see why these restrictions can be necessary, consider an example wherein we are trying to establish that an x-correlated sample in $G_1 \oplus G_2$ is indistinguishable from a random sample in $G_1 \oplus G_2$ for a known x. Suppose we are given generators h_1 and h_2. If we are given an x-correlated sample $g_1^\alpha g_2^{\alpha x}$ (for some random, unknown α), we can then compute $e(g_1, h_1)^\alpha$ and $e(g_2, h_2)^{\alpha x}$. When we are working with specific instantiations, it may be the case that that there is a known relationship between the values $e(g_1, h_1)$ and $e(g_2, h_2)$ in the target group. (In fact, for our IBE construction, we will have $e(g_1, h_1) = e(g_2, h_2)^{-1}$.) In such a case, we can use our knowledge of x to test for an x-correlation in the target group, and hence distinguish if we were given an x-correlated sample or a random one. Similarly, if we have this same relationship in the target group and we have x-correlated samples on both sides, $g_1^\alpha g_2^{\alpha x}$ and $h_1^{\beta x} h_2^\beta$, then pairing these yields the identity in the target group, hence distinguishing these from two random samples.

Definition 2.6 (Parameter hiding)**.** *We say that a group $\mathbb{G} = (N, G, H, G_T, e, \mu)$ satisfies* parameter hiding *if for all $k_3, \ell_3 \in \mathbb{N}$, sets $X \in (\mathbb{Z}/N\mathbb{Z})^{k_3}$ and $Y \in (\mathbb{Z}/N\mathbb{Z})^{\ell_3}$, and distributions $\mathcal{D} = (S_G, S_H, X, Y, C)$ that are well-behaved in the above sense, $\mathcal{D}$ is identical to the distribution in which the correlated samples indicated by C are replaced with random samples.*

Example 2.7. As an example, consider the distribution $\mathcal{D}$ defined by $S_G = \{1, 2; ; (1, 2), (3, 4)\}$, $S_H = \{1, 2, 5, 6; (3, 4), (3, 4); (1, 2), (3, 4)\}$, $C = \{(3, 4); (3, 4)\}$, $X = \{x\}$, and $Y = \{y\}$ for any $x, y \in \mathbb{Z}/N\mathbb{Z}$ such that $x \neq y$; we can easily check that these sets are well-behaved in the sense defined above. Then parameter hiding holds for $\mathbb{G} = (N, G, H, G_T, e, \mu)$ if for $a, b, c, d, s, t, u, v, w, z \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ we have that

$$(N, G, H, G_T, e, \mu, g_1, g_2, h_1, h_2, h_5, h_6, h_3^a h_4^b, h_3^c h_4^d, h_1^{ty} h_2^t, h_3^{zy} h_4^z, g_1^s g_2^{sx}, g_3^w g_4^{wx})$$

is *identical* to

$$(N, G, H, G_T, e, \mu, g_1, g_2, h_1, h_2, h_5, h_6, h_3^a h_4^b, h_3^c h_4^d, h_1^{ty} h_2^t, h_3^v h_4^z, g_1^s g_2^{sx}, g_3^w g_4^u).$$

In our uses of parameter hiding in Section 4, we restrict ourselves to this one example. Again, this is due to the difficulty of providing a fully general definition of parameter hiding as certain types of correlated samples require more entropy than others; for example, if we wanted to switch from $h_3^{zy} h_4^z$ and $g_3^w g_4^{wx}$, and then additionally from $g_3^v g_4^{vx'}$, it would not be clear how to do this with the usual tricks, since these use the ambiguity in the choice of generators for G_3, G_4, H_3, H_4, which only provides a fixed amount of entropy. There would be several approaches to deal with such an issue in a particular application, like expanding G_3, G_4, H_3, H_4 internally to consist of several further subgroups (thereby providing more entropy) or using a hybrid argument to avoid the necessity of switching so many samples at once. We do not find it to be overly limiting to consider this one example, in which we switch from correlated to random samples in only the spaces $G_3 \oplus G_4$ and $H_3 \oplus H_4$, to keep our constructions in Section 4 simple and tailored to the requirements that we need.

2.3 Generalized correlated subgroup decision

Beyond functional properties of bilinear groups, we must also consider the types of security guarantees we can provide. The assumption we define, generalized correlated subgroup decision, considers indistinguishability between subgroups in a very general way: given certain subgroup generators and "correlated" elements across subgroups (i.e., elements in different subgroups that use the same randomness), we require that it should still be hard to distinguish between elements of other subgroups. Formally, we consider sets $S_G = (s_1, \ldots, s_{k_1}; t_1, \ldots, t_{\ell_1})$, $S_H = (s'_1, \ldots, s'_{k_2}; t'_1, \ldots, t'_{\ell_2})$, $T_1 = \{(p_1, \pi_1), \ldots, (p_m, \pi_m)\}$, and $T_2 = \{(p'_1, \pi'_1), \ldots, (p'_{m+1}, \pi'_{m+1})\}$, and an indicator bit b. (We assume without loss of generality that T_2 is the larger set.) Intuitively, the sets S_G and S_H tells us which group elements an adversary is given, and (T_1, T_2, b) tell us what the challenge terms should look like. We have the following requirements for S_G:

- Each singleton $s_i \in S_G$ indicates that we are given the generators g_{s_i}.
- Each tuple $t_i = (P_{1,i} = (p_{1,i}, \pi_{1,i}), \ldots, P_{m,i} = (p_{m,i}, \pi_{m,i}))$ of pairs of primes in S_G indicates that we are given values $g_{p_{1,i}}^{a_1} \cdot \ldots \cdot g_{p_{m,i}}^{a_m}$ and $g_{\pi_{1,i}}^{a_1} \cdot \ldots \cdot g_{\pi_{m,i}}^{a_m}$ for $a_1, \ldots, a_m \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$; i.e., for each i, we are given a pair of products: the first consisting of random elements in each of the subgroups of G indicated by the first component of the pair, and the second consisting of random elements in each of the subgroups of G indicated by the second component of the pair. Note that these elements are *correlated*, in that the same randomness is used for both. For convenience, we will restrict to pairs $(p_{k,i}, \pi_{k,i})$ such that $p_{k,i}$ is odd and $\pi_{k,i} = p_{k,i} + 1$ (i.e. all pairs are chosen among (1,2), (3,4), (5,6), etc.)
- The bit b indicates which group the challenge element comes from: $b = 0$ indicates G, and $b = 1$ indicates H.
- For the sets T_1 and T_2, we require that they differ in exactly one pair; i.e., there exists a unique pair P such that $P \notin T_1$ but $P \in T_2$. For this pair $P = (p, \pi)$, we require that $s_i \neq p$ and $s_i \neq \pi$ for any $s_i \in S_G$ or $s_i \in S_H$; i.e., we are not given the generators for these subgroups on either side of the pairing, and also that if $P \in t_i$ for some i (for either $t_i \in S_G$ or $t_i \in S_H$), then we must have $T_1 \cap t_i \neq \emptyset$; i.e., P can appear only in tuples in S_G or S_H that also contain another component in the challenge term. As in sets S_G and S_H, we require that all pairs appearing in T_1, T_2 are elements of $\{(1,2), (3,4), (5,6), \ldots\}$. Then, assuming $b = 0$ (and replacing g with h if $b = 1$), our challenge elements are of the form $T := (g_{p_1}^{a_1} \cdot \ldots \cdot g_{p_m}^{a_m}, g_{\pi_1}^{a_1} \cdot \ldots \cdot g_{\pi_m}^{a_m})$ and $T' := (g_{p_{1'}}^{a_1} \cdot \ldots \cdot g_{p'_{m+1}}^{a_{m+1}}, g_{\pi'_1}^{a_1} \cdot \ldots \cdot g_{\pi'_{m+1}}^{a_{m+1}})$ for $a_1, \ldots a_{m+1} \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$.

Assumption 2.8 (Generalized correlated subgroup decision)**.** *For all tuples (S_G, S_H, T_1, T_2, b) satisfying the requirements specified above and for any $n \in \mathbb{N}$, for any PPT adversary $\mathcal{A}$ given $\mathbb{G} \xleftarrow{\$}$ $\mathsf{BilinearGen}(1^k, n)$ and the elements specified by S_G and S_H, it should be hard to distinguish between values T defined by (b, T_1) and values T' defined by (b, T_2).*

As an example, consider the case in which $n = 6$ and $S_G = \{1, 2; ((1,2), (3,4))\}$, $S_H = \{1, 2, 5, 6; ((1,2), (3,4)), ((3,4), (5,6))\}$, $T_1 = \{(1,2), (5,6)\}$, $T_2 = \{(1,2), (3,4), (5,6)\}$, and $b = 0$. In this case, the concrete assumption is: Given $\mathbb{G}$ and generators $g_1, g_2, h_1, h_2, h_5, h_6$, correlated samples from $G_1 \oplus G_3$ and $G_2 \oplus G_4$, correlated samples from $H_1 \oplus H_3$ and $H_2 \oplus H_4$, and correlated samples from $H_3 \oplus H_5$ and $H_4 \oplus H_6$, it should be hard to distinguish correlated samples from $G_1 \oplus G_5$ and $G_2 \oplus G_6$ from correlated samples from $G_1 \oplus G_3 \oplus G_5$ and $G_2 \oplus G_4 \oplus G_6$.

3 A Prime-Order Bilinear Group Satisfying All Features

Our ultimate goal in this section is to define a prime-order bilinear group that satisfies all three of the properties defined in the previous section: projecting, canceling, and parameter hiding; additionally, we want to require that subgroup decision is hard in this group. Our construction can be viewed as an abstraction of the construction of Seo and Cheon [30], which they prove satisfies (regular) projecting, canceling, and a somewhat restrictive notion of subgroup decision. In contrast, our construction satisfies canceling and parameter hiding, is flexible enough to achieve any of the three flavors of projecting we defined in the previous section (depending on the parameter choices), and comes equipped with reductions for more general instances of subgroup decision.

Notationally, we augment the bilinear groups $\mathbb{G}$ discussed in the previous section. In particular, we now focus only on the case when the group order is some prime p, and consider groups $\mathbb{B} = (p, B_1, B_2, B_T, E, \mu)$ built on top of groups $\mathbb{G} = (p, G, H, G_T, e)$; this means B_1, B_2, and B_T may contain multiple copies of G, H, and G_T respectively (formally, B_1, B_2, and B_T are all $\mathbb{F}_p$-modules), and that the map E uses e as a component. Because we are moving to these bigger spaces, we must also include a value μ that allows us to test membership in the groups B_1 and B_2; as an example, consider the case in which $B_1 \subset G \times G$ and one can test for membership in G. Then, while it is easy to test for membership in $G \times G$, we must give out additional information μ that allows one to (efficiently) test for membership in B_1.

Our construction crucially uses dual pairing vector spaces, which were introduced by Okamoto and Takashima [25, 26] and have been previously used to provide pairings $E : G^n \times H^n \to G_T$, built on top of pairings $e : G \times H \to G_T$, that satisfy the canceling property. As we cannot have a cyclic target space if we want to satisfy projecting or full projecting, however, we instead need a map whose image is G_T^d for some d that can be larger than 1. Intuitively, we achieve this by piecing together d "blocks," where each block is an instance of a dual pairing vector space; the construction of Seo and Cheon is then obtained as the special case in which $d = n$, and dual pairing vector spaces as defined by Okamoto and Takashima are obtained with $d = 1$. More formally, we begin with a key definition:

Definition 3.1 (Dual orthonormal). *Two bases* $\mathbb{B} := (\vec{b}_1, \ldots, \vec{b}_n)$ *and* $\mathbb{B}^* := (\vec{b}_1^*, \ldots, \vec{b}_n^*)$ *of* $\mathbb{F}_p^n$ *are* dual orthonormal *if* $\vec{b}_j \cdot \vec{b}_j^* \equiv 1 \bmod p$ *for all* j, $1 \le j \le n$, *and* $\vec{b}_j \cdot \vec{b}_k^* \equiv 0 \bmod p$ *for all* $j \neq k$.

We note that one can efficiently sample a random pair of dual orthonormal bases $(\mathbb{B}, \mathbb{B}^*)$ by sampling first a random basis $\mathbb{B}$ and then solving uniquely for $\mathbb{B}^*$ using linear algebra over $\mathbb{F}_p$; we denote this sampling process as $(\mathbb{B}, \mathbb{B}^*) \xleftarrow{\$} Dual(\mathbb{F}_p^n)$. By repeating this sampling process d times, we can obtain a tuple $((\mathbb{B}_1, \mathbb{B}_1^*), \ldots, (\mathbb{B}_d, \mathbb{B}_d^*))$ of d pairs of dual orthonormal bases of $\mathbb{F}_p^n$. We denote the vectors of $\mathbb{B}_i$ as $(\vec{b}_{1,i} \ldots, \vec{b}_{n,i})$, and the vectors of $\mathbb{B}_i^*$ as $(\vec{b}_{1,i}^*, \ldots, \vec{b}_{n,i}^*)$. We then give the following definition:

Definition 3.2 (Concatenation). *The* concatenation *of bases* $(\mathbb{B}_1, \ldots, \mathbb{B}_d)$ *of* $\mathbb{F}_p^n$ *is a collection of* n *vectors* $(\vec{v}_1, \ldots, \vec{v}_n)$ *in* $\mathbb{F}_p^{dn}$, *where each* $\vec{v}_j := \vec{b}_{j,1} || \ldots || \vec{b}_{j,d}$. *Alternatively, we can view each* $\vec{v}_j$ *as a* $d \times n$ *matrix, where the* i*-th row is* $\vec{b}_{j,i}$. *We denote the concatenation of* $(\mathbb{B}_1, \ldots, \mathbb{B}_d)$ *as* $\mathsf{Concat}(\mathbb{B}_1, \ldots, \mathbb{B}_d)$.

To begin our construction, we build off of a group $\mathbb{G} = (p, G, H, G_T, e, g, h)$, where g and h are generators of G and H respectively, and consider groups $B_1 \subset G^{dn}$ and $B_2 \subset H^{dn}$. Notationally, we write an element of B_1 as g^A, where $A = (\alpha_{i,j})_{i,j=1}^{d,n}$ is a $d \times n$ matrix and $g^A := (g^{\alpha_{1,1}}, \ldots, g^{\alpha_{1,j}}, \ldots, g^{\alpha_{1,n}}, g^{\alpha_{2,1}}, \ldots, g^{\alpha_{d,n}})$. We similarly write elements of B_2 as h^B for a $d \times n$ matrix $B = (\beta_{ij})_{i,j=1}^{d,n}$, and furthermore define the bilinear map $E : B_1 \times B_2 \to G_T^d$ as

$$E(g^A, h^B) := \left(\prod_{k=1}^{n} e(g^{\alpha_{1,k}}, h^{\beta_{1,k}}), \ldots, \prod_{k=1}^{n} e(g^{\alpha_{d,k}}, h^{\beta_{d,k}}) \right). \quad (1)$$

Observe that the i-th coordinate of the image is equal to $e(g, h)^{A_i \cdot B_i \bmod p}$, where A_i and B_i denote the i-th rows of A and B respectively. Then, to begin to see how our construction will satisfy projecting and canceling, we have the following lemma:

Lemma 3.3. *Let* $(\vec{v}_1, \ldots, \vec{v}_n) = \mathsf{Concat}(\mathbb{B}_1, \ldots, \mathbb{B}_d)$ *and* $(\vec{v}_1^*, \ldots, \vec{v}_n^*) = \mathsf{Concat}(\mathbb{B}_1^*, \ldots, \mathbb{B}_d^*)$, *where* $(\mathbb{B}_i, \mathbb{B}_i^*)$ *are dual orthonormal bases of* $\mathbb{F}_p^n$. *Then*

$$E(g^{\vec{v}_j}, h^{\vec{v}_j^*}) = (e(g, h), \ldots, e(g, h)) \ \forall j \quad \textit{and} \quad E(g^{\vec{v}_j}, h^{\vec{v}_k^*}) = (1_T, \ldots, 1_T) \ \forall j \neq k.$$

Proof. By the definition of the pairing, we have for any j and k that

$$E(g^{\vec{v}_j}, h^{\vec{v}_k^*}) = \left(e(g,h)^{\vec{b}_{j,1}\cdot\vec{b}_{k,1}^*}, \dots, e(g,h)^{\vec{b}_{j,d}\cdot\vec{b}_{k,d}^*}\right).$$

If $j = k$, then the fact that $(\mathbb{B}_i, \mathbb{B}_i^*)$ are dual orthonormal for all i implies by definition that $\vec{b}_{j,i} \cdot \vec{b}_{j,i}^* \equiv 1 \bmod p$ for all i and j, and thus $E(g^{\vec{v}_j}, h^{\vec{v}_j^*}) = (e(g,h), \dots, e(g,h))$. For the second property, we again use the definition of dual orthonormal bases to see that $\vec{b}_{j,i} \cdot \vec{b}_{k,i}^* \equiv 0 \bmod p$ for all $j \neq k$, and thus $E(g^{\vec{v}_j}, h^{\vec{v}_k^*}) = (1_T, \dots, 1_T)$. □

While Lemma 3.3 therefore shows us directly how to obtain canceling, for projecting we are still mapping into a one-dimensional image. To obtain more dimensions, it turns out we need only perform some additional scalar multiplication. We give the following definition:

Definition 3.4 (Scaling)**.** *Define $C = (c_{i,j})_{i,j=1}^{d,n}$ to be a $n \times d$ matrix over $\mathbb{F}_p$. Given bases $(\mathbb{B}_1, \dots, \mathbb{B}_d)$ of $\mathbb{F}_p^n$, we define the* scaling *of these bases by C to be new bases $(\mathbb{D}_1, \dots, \mathbb{D}_d)$, where $\mathbb{D}_i = (c_{1,i}\vec{b}_{1,i}, \dots, c_{n,i}\vec{b}_{n,i})$ for all i, $1 \leq i \leq d$. We denote the scaling of $(\mathbb{B}_1, \dots, \mathbb{B}_d)$ by C as $\mathsf{Scale}(C, \mathbb{B}_1, \dots, \mathbb{B}_d)$.*

Intuitively then, we use the entries in the i-th column of C to scale the vectors in the basis $\mathbb{B}_i$ and obtain the basis $\mathbb{D}_i$. We observe that, as we still have $\vec{b}_{j,i} \cdot \vec{b}_{k,i}^* \equiv 0 \bmod p$ for $j \neq k$, multiplication by a scalar will not affect this and we still satisfy canceling. The scalar values do, however, build in extra dimensions into the image of our pairing, as demonstrated by the following lemma:

Lemma 3.5. *Let $(\mathbb{B}_1, \dots, \mathbb{B}_d)$ and $(\mathbb{B}_1^*, \dots, \mathbb{B}_d^*)$ be sets of bases for $\mathbb{F}_p^n$ such that $(\mathbb{B}_i, \mathbb{B}_i^*)$ are dual orthonormal for all i. Define $(\vec{v}_1, \dots, \vec{v}_n) := \mathsf{Concat}(\mathbb{D}_1, \dots, \mathbb{D}_d)$ and $(\vec{v}_1^*, \dots, \vec{v}_n^*) := \mathsf{Concat}(\mathbb{B}_1^*, \dots, \mathbb{B}_d^*)$, where $(\mathbb{D}_1, \dots, \mathbb{D}_d) = \mathsf{Scale}(C, \mathbb{B}_1, \dots, \mathbb{B}_d)$ for some $C \in M_{n\times d}(\mathbb{F}_p)$. Then*

$$E(g^{\vec{v}_j}, h^{\vec{v}_j^*}) = (e(g,h)^{c_{j,1}}, \dots, e(g,h)^{c_{j,d}})\ \forall j \quad \textit{and} \quad E(g^{\vec{v}_j}, h^{\vec{v}_k^*}) = (1_T, \dots, 1_T)\ \forall j \neq k.$$

Proof. By the definition of the pairing, we have for any j and k that

$$E(g^{\vec{v}_j}, h^{\vec{v}_k^*}) = \left(e(g,h)^{c_{j,1}\vec{b}_{j,1}\cdot\vec{b}_{k,1}^*}, \dots, e(g,h)^{c_{j,d}\vec{b}_{j,d}\cdot\vec{b}_{k,d}^*}\right).$$

If $j = k$, then the fact that $(\mathbb{B}_i, \mathbb{B}_i^*)$ are dual orthonormal for all i implies by definition that $\vec{b}_{j,i} \cdot \vec{b}_{j,i}^* \equiv 1 \bmod p$ for all i and j, and thus $c_{j,i}\vec{b}_{j,i}\cdot\vec{b}_{j,i}^* \equiv c_{j,i} \bmod p$ and $E(g^{\vec{v}_j}, h^{\vec{v}_j^*}) = (e(g,h)^{c_{j,1}}, \dots, e(g,h)^{c_{j,d}})$. For the second property, we again use the definition of dual orthonormal bases to see that $\vec{b}_{j,i}\cdot\vec{b}_{k,i}^* \equiv 0 \bmod p$ for all $j \neq k$, and thus $c_{j,i}\vec{b}_{j,i} \cdot \vec{b}_{k,i}^* \equiv 0 \bmod p$ and $E(g^{\vec{v}_j}, h^{\vec{v}_k^*}) = (1_T, \dots, 1_T)$. □

We are now ready to give our full construction of an algorithm $\mathsf{BilinearGen}'$, parameterized by integers n and d, and a distribution $\mathcal{D}_{n,d}$ on $n \times d$ matrices, to achieve a setting $\mathbb{B} = (p, B_1, B_2, B_T, E, \mu)$ such that $B_1 \subset G^{dn}$, $B_2 \subset H^{dn}$, and $B_T = G_T^d$. We present this construction in Algorithm 1, and demonstrate that it satisfies projecting, canceling, parameter hiding, and subgroup decision.

The generality of this construction stems from the choices of d, n, and $\mathcal{D}$; in fact, by choosing different values for these parameters, we can satisfy each of the different flavors of projecting from Section 2. To satisfy fully projecting, we must choose C from a distribution supported on matrices of full rank n and have $d \geq n$. If we use a less restrictive distribution, we obtain weaker projection capabilities and a more efficient construction (as we can have $d < n$) when projecting onto all subgroups individually is not needed: to achieve (regular) projecting, we can use $d > 1$ and pick C to be of rank > 1, and to achieve weak projecting we can in fact use $d = 1$ and pick C to be the vector consisting of all 1 entries.

Algorithm 1 BilinearGen$'$: generate a bilinear group $\mathbb{B}$ that satisfies projecting and canceling

Input: $d, n \in \mathbb{N}$; distribution $\mathcal{D}_{d,n}$ over matrices in $M_{n\times d}(\mathbb{F}_p)$; security parameter 1^k.

1. $(p, G, H, G_T, e) \xleftarrow{\$} \mathsf{BilinearGen}(1^k, 1)$.
2. Pick values g and h such that $G = \langle g \rangle$ and $H = \langle h \rangle$.
3. Sample d pairs $(\mathbb{B}_i, \mathbb{B}_i^*) \xleftarrow{\$} \mathit{Dual}(\mathbb{F}_p^n)$ to obtain two sets $(\mathbb{B}_1, \ldots, \mathbb{B}_d)$ and $(\mathbb{B}_1^*, \ldots, \mathbb{B}_d^*)$ of bases of $\mathbb{F}_p^n$, where $(\mathbb{B}_i, \mathbb{B}_i^*)$ are dual orthonormal.
4. Sample $C = (c_{ij})_{i,j=1}^{d,n} \xleftarrow{\$} \mathcal{D}$ and compute $(\mathbb{D}_1, \ldots, \mathbb{D}_d) := \mathsf{Scale}(C, \mathbb{B}_1, \ldots, \mathbb{B}_d)$.
5. For all i, $1 \le i \le n$, define $B_{1,i} := \langle g^{\vec{v}_i} \rangle$ and $B_{2,i} := \langle h^{\vec{v}_i^*} \rangle$, where $(\vec{v}_1, \ldots, \vec{v}_n) := \mathsf{Concat}(\mathbb{D}_1, \ldots, \mathbb{D}_d)$ and $(\vec{v}_1^*, \ldots, \vec{v}_n^*) := \mathsf{Concat}(\mathbb{B}_1^*, \ldots, \mathbb{B}_d^*)$.
6. Define $B_1 := \oplus_{i=1}^n B_{1,i} \subset G^{dn}$, $B_2 := \oplus_{i=1}^n B_{2,i} \subset H^{dn}$, and $B_T := G_T^d$. Define the pairing $E : B_1 \times B_2 \to B_T$ as in Equation 1.
7. Finally, to be able to check that an element $g^M \in G^{dn}$ for $M = (m_{ij})_{i,j=1}^{d,n}$ is an element of B_1, we observe that the vectors $\vec{v}_1, \ldots, \vec{v}_n$ span an n-dimensional subspace $\mathbb{V}$ of $\mathbb{F}_p^{dn}$. Thus, there must be another subspace, call it $\mathbb{W}$, of dimension $dn - n$, that contains all vectors in $\mathbb{F}_p^n$ that are orthogonal to vectors in $\mathbb{V}$. Given $\mu_2 := (h^{\vec{w}_1}, \ldots, h^{\vec{w}_{(d-1)n}})$, where the $\{\vec{w}_i\}_{i=1}^{(d-1)n}$ are a basis of $\mathbb{W}$, one can therefore efficiently check if $g^M \in B_1$ by checking if $E(g^M, h^{\vec{w}_i}) = (1_T, \ldots, 1_T)$ for all i, $1 \le i \le (d-1)n$. Analogously, given $\mu_1 := (g^{\vec{w}_1^*}, \ldots, g^{\vec{w}_{(d-1)n}^*})$, one can check if $h^A \in B_2$ by checking if $E(g^{\vec{w}_i^*}, h^A) = (1_T, \ldots, 1_T)$, where $\{\vec{w}_i^*\}_{i=1}^{(d-1)n}$ are a basis for the subspace $\mathbb{W}^*$ of $\mathbb{F}_p^n$ consisting of vectors orthogonal to vectors in the span of $\vec{v}_1^*, \ldots, \vec{v}_n^*$.
8. Output $\mathbb{B} := (p, B_1, B_2, B_T, E, (\mu_1, \mu_2))$.

Theorem 3.6. *For all values of $n \ge 2$, the bilinear group $\mathbb{B} \xleftarrow{\$} \mathsf{BilinearGen}'(1^k, n, d)$ satisfies canceling, fully projecting as defined in Definition 2.3 for $d \ge n$ when C has full rank, projecting as defined in Definition 2.2 for $d > 1$ when C has rank > 1, and weak projecting as defined in Definition 2.1 for $d = 1$.*

Proof. Given that our construction was specifically designed to satisfy the conditions for Lemma 3.5, we immediately obtain canceling. To satisfy projecting, we additionally need to construct the projection maps π_{ij} and argue that they satisfy the requirements of Definition 2.3 (in the case that C is full rank). By the way our subgroups are defined, each projection map π_{1i} within the group B_1 must map an arbitrary element $g^{a_1\vec{v}_1 + \cdots + a_n\vec{v}_n}$ of B_1 to $g^{a_i\vec{v}_i} \in B_{1,i}$; similarly, π_{2i} must map $h^{a_1^*\vec{v}_1^* + \cdots + a_n^*\vec{v}_n^*} \in B_2$ to $h^{a_i^*\vec{v}_i^*} \in B_{2,i}$. For π_{1i}, we observe that it can be computed efficiently by anyone knowing $\vec{v}_i$ and another vector in $\mathbb{F}_p^{dn}$ that is orthogonal to $\vec{v}_k$ for all $k \ne i$. The situation for π_{2i} is analogous.

As for the projection maps $\pi_{T,i}$ required for the target space, we define $\pi_{T,i}$ to map an element $e(g,h)^{a_1C_1 + \cdots + a_nC_n}$ to $e(g,h)^{a_iC_i}$, where we recall C_i denotes the i-th row of the scaling matrix C (C_i is thus a vector in $\mathbb{F}_p^d$ for all i).

Finally, we show that the required associativity property holds, namely that $E(\pi_{1,i}(g^M), \pi_{2,i}(h^A)) = \pi_{T,i}(E(g^M, h^A))$ for all elements $g^M \in B_1$, $h^A \in B_2$, and for all i, $1 \le i \le d$. To see this, observe that $g^M \in B_1$ implies that $g^M = g^{\alpha_1\vec{v}_1 + \cdots + \alpha_n\vec{v}_n}$ for some $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_p$, and similarly that $h^A = h^{\beta_1\vec{v}_1^* + \cdots + \beta_n\vec{v}_n^*}$. We therefore have that

$$E(\pi_{1,i}(g^M), \pi_{2,i}(h^A)) = E(g^{\alpha_i\vec{v}_i}, h^{\beta_i\vec{v}_i^*}) = e(g,h)^{\alpha_i\beta_iC_i},$$

where this last equality follows from Lemma 3.5. On the other hand, we have that

$$\pi_{T,i}(E(g^M, h^A)) = \pi_{T,i}(\prod_{k=1}^{n} e(g,h)^{\alpha_k\beta_kC_k}) = e(g,h)^{\alpha_i\beta_iC_i},$$

and the two quantities are therefore equal.

A similar argument applies to obtaining more limited projections when C has lower rank. □

As discussed in Section 2, the definitions we provide for the other two desirable properties — parameter hiding and hardness of subgroup decision — are both highly general. To ease exposition, we therefore focus on establishing these properties for only the specific instances we need in Section 4, although these are by no means the only instances for which parameter hiding and subgroup decision hold. This means restricting our attention to the case where $n = 8$, $d = 1$, C is a matrix with all 1 entries. For succinctness here and in later sections, we use $\mathsf{BasicGen}(1^k) = \mathsf{BilinearGen}'(1^k, 8, 1, \mathcal{D})$, where $\mathcal{D}$ produces matrices with all 1 entries; i.e., we use BasicGen to produce the specific setting in which we are interested.

We consider two variants of this setting, which differ only in the auxiliary information μ. For μ as defined above in Algorithm 1, we show that the required instances of the correlated subgroup decision assumption are implied by SXDH. We additionally consider a case where μ is augmented to contain the following three pieces of information: (1) the vectors $\vec{v}_7$, $\vec{v}_8$, $\vec{v}_7^*$, and $\vec{v}_8^*$; (2) a random basis for the span of $(\vec{v}_1, \dots, \vec{v}_6)$ inside $\mathbb{F}_p^8$; and (3) a random basis for the span of $(\vec{v}_1^*, \dots, \vec{v}_6^*)$ inside $\mathbb{F}_p^8$. With this μ, one can then perform a membership test for $G_1 \oplus \dots \oplus G_6$ on some element $g^{\vec{v}}$ by computing a basis for the orthogonal space of the span of $(\vec{v}_1, \dots, \vec{v}_6)$, pairing against h raised to these vectors, and taking a dot product in $\mathbb{F}_p^8$. While this additional information in μ makes some instances of subgroup decision easy, instances entirely within $G_1 \oplus \dots \oplus G_6$ and $H_1 \oplus \dots H_6$ are still implied by SXDH. To refer to this instance with augmented μ in what follows, we will call it the *augmented construction*.

Lemma 3.7. *Parameter hiding, as in Example 2.7, holds for the augmented construction.*

Proof. This is essentially Lemmas 3 and 4 in [18], and is a consequence of the following observation. We consider sampling a random pair of dual orthonormal bases $\mathbb{F}, \mathbb{F}^*$ of $\mathbb{F}_p^8$, and let A be an invertible 2×2 matrix over $\mathbb{F}_p$. We consider the 8×2 matrix F whose columns are equal to $\vec{f}_3$ and $\vec{f}_4$. Then FA is also an 8×2 matrix, and we form a new basis $\mathbb{B}$ from $\mathbb{F}$ and A by taking these columns in place of $\vec{f}_3, \vec{f}_4$. To form the dual basis $\mathbb{B}^*$, we similarly multiply the matrix with columns $\vec{f}_3^*, \vec{f}_4^*$ by the transpose of A^{-1}. It is noted in [18] that the resulting distribution of $\mathbb{B}, \mathbb{B}^*$ is equivalent to choosing this pair randomly, and in particular, this distribution is independent of the choice of A. Lemma 4 in [18] observes that if take $x \neq y$ and define $\vec{x}$ to be the transpose of $(1, x)$ and $\vec{y}$ to the be transpose of $(y, -1)$, then choosing random scalars γ, λ in $\mathbb{F}_p$ and a random matrix A over $\mathbb{F}_p$ yields that the joint distribution of $\lambda A^{-1}\vec{x}$ and $\gamma A^T \vec{y}$ is negligibly close to the uniform distribution over $\mathbb{F}_p^2 \times \mathbb{F}_p^2$. This is precisely our parameter hiding requirement, where A represents the ambiguity in our precise choice of the generators $\vec{b}_3, \vec{b}_4, \vec{b}_3^*, \vec{b}_4^*$, conditioned on the span of $\{\vec{b}_3, \vec{b}_4\}$ and the span of $\{\vec{b}_3^*, \vec{b}_4^*\}$ being known (in addition to the other individual $\vec{b}_i$ and $\vec{b}_i^*$ vectors for $i \notin \{3, 4\}$). □

We now show — again restricting our attention to the BasicGen setting — that certain "nice" instances of the generalized correlated subgroup decision assumption follow from SXDH. By "nice," we mean that the instance of the assumption behaves as follows: if the challenge terms are in H (the situation is analogous if they are in G), then there is a single pair in S that is common to the challenge sets T_1 and T_2 that appears in all tuples in S_G that also contain the differing pair. In other words, the given correlated samples from the opposite side of the challenge that include the differing space must also be attached to a particular space that is guaranteed to be present in the challenge term. As we will see, this feature turns out to be convenient for reducing to SXDH, as demonstrated by the following lemmas. For the augmented construction, we additionally restrict to instances where each correlated sample t_i in S_G or S_H is contained within the set $S := \{(1,2), (3,4), (5,6)\}$ (this is to avoid the additional information in μ from compromising the hardness).

Lemma 3.8. *For the augmented construction, the nice instances of the generalized correlated subgroup decision assumption, where additionally each correlated sample t_i in S_G or S_H is contained within the set $\{(1,2),(3,4),(5,6)\}$, are implied by the SXDH assumption.*

Proof. We consider a nice instance of the generalized correlated subgroup decision assumption parameterized by sets S_G and S_H containing singletons and tuples of the pairs $(1,2)$, $(3,4)$, $(5,6)$ and challenge sets T_1 and T_2 differing by one pair. We assume without loss of generality that the differing pair is $(3,4)$, that $(1,2)$ is a common pair to both T_1, T_2, and the challenge terms are in G.

We assume we are given an SXDH challenge of the form (g, h, g^a, g^b, T), where $T = g^{ab}$ or is random in G. We will simulate the specified instance of the generalized correlated subgroup decision assumption. We first choose a random dual orthonormal bases pair $\mathbb{F}, \mathbb{F}^*$ for $\mathbb{F}_p^8$. We then implicitly define $\mathbb{B}, \mathbb{B}^*$ as follows:

$$\vec{b}_1 = a\vec{f}_3 + \vec{f}_1,\ \vec{b}_2 = a\vec{f}_4 + \vec{f}_2,\ \vec{b}_3 = \vec{f}_3,\ \vec{b}_4 = \vec{f}_4,\ \vec{b}_5 = \vec{f}_5,\ \vec{b}_6 = \vec{f}_6,\ \vec{b}_7 = \vec{f}_7,\ \vec{b}_8 = \vec{f}_8$$

$$\vec{b}^*_1 = \vec{f}^*_1,\ \vec{b}^*_2 = \vec{f}^*_2,\ \vec{b}^*_3 = \vec{f}^*_3 - a\vec{f}^*_1,\ \vec{b}^*_4 = \vec{f}^*_4 - a\vec{f}^*_2,\ \vec{b}^*_5 = \vec{f}^*_5,\ \vec{b}^*_6 = \vec{f}^*_6,\ \vec{b}^*_7 = \vec{f}^*_7,\ \vec{b}^*_8 = \vec{f}^*_8.$$

We note that $(\mathbb{B}, \mathbb{B}^*)$ are properly distributed, since applying a linear transformation to randomly sampled dual orthonormal bases while preserving orthonormality produces equivalently distributed bases. We observe that $\vec{v}_7, \vec{v}_8, \vec{v}^*_7, \vec{v}^*_8$ are known, as are the spans of $\{\vec{v}_1, \ldots, \vec{v}_6\}$ and $\{\vec{v}^*_1, \ldots, \vec{v}^*_6\}$. Thus we can produce the specified auxiliary information μ.

Since we have h, g, g^a, we can produce all generators *except* h_3, h_4. Since $(3,4)$ is the differing pair for the challenges, these generators cannot be required. Since all generators are known on the G side, any correlated samples in G are easy to produce. To produce correlated samples for tuples containing $(1,2)$ and $(3,4)$ in H, we simply choose random exponents $t', z \in \mathbb{Z}_p$ and implicitly set $t = az + t'$. We can then produce

$$h_1^t h_3^z = h^{t'\vec{f}^*_1 + z\vec{f}^*_3},\ h_2^t h_4^z = h^{-t'\vec{f}^*_2 - z\vec{f}^*_4}.$$

To produce the challenge terms, we compute

$$T^{\vec{f}_3}(g^b)^{\vec{f}_1},\ T^{\vec{f}_4}(g^b)^{\vec{f}_2}.$$

If $(5,6)$ is also common to T_1, T_2, we can use the generators g_5, g_6 to add on properly distributed terms in these subgroups as well. □

The same proof can also be applied more generally when μ is *not* augmented, resulting in:

Lemma 3.9. *For $\mathbb{G} \xleftarrow{\$} \mathsf{BasicGen}(1^k)$, all nice instances of the generalized correlated subgroup decision assumption are implied by SXDH.*

Although we do not use any non-nice instances of the generalized correlated decision assumption in this work, it is interesting to ask which of the more complex instances can be reduced to SXDH or other static assumptions. For values of $d > 1$, the additional structure required to achieve projecting seems to make reducing to SXDH difficult. For these cases, reducing to other static assumptions with more structure than SXDH (having higher degree relationships between exponent variables, for example) is much easier, and we do not know if reducing all the way down to SXDH is achievable or not. We leave this as an interesting question for future work.

4 An IBE with IND-CCA1 Security

With our bilinear setting in place, we now consider how to make use of the properties it simulates; i.e., explore what benefits the combination of projecting, canceling, parameter hiding, and subgroup decision yields. As mentioned in the introduction, the application we provide is an IND-CCA1-secure identity-based encryption scheme. Although IND-CCA2-secure IBE schemes have already been constructed, we believe our techniques are more generally useful beyond this single application.

At its heart, our construction can be thought of as a variant on the Boneh-Boyen scheme, which is IND-CPA secure (and is clearly not IND-CCA2 secure, as it has re-randomizable ciphertexts). By adding in various components in different subgroups, we first show (using canceling, parameter hiding, and subgroup decision variants) that our construction satisfies a weak notion of IND-CCA1 security, in which the adversary does not even get to see the public parameters. While such a notion might not seem to be very useful on its own, we next show that, by folding in weak projecting for additional subgroups, we are able to boost up to full IND-CCA1 security. This is a new application of projecting that requires only a mild expansion of the structure of the original scheme and fits in nicely with the evolution of dual system encryption techniques.

The high-level idea of the construction and proof is as follows. We start with the core Boneh-Boyen construction and embed it into groups with several canceling subgroups; we then add decryption checks to confirm that the ciphertext conforms to the appropriate structure in certain subgroups. Now, we observe that if an adversary is not given the public parameters, it can attempt to produce well-formed decryption queries only using the information it gains from key requests. We can apply a dual-system encryption approach to add random components to these keys in a subgroup that we also add to the ciphertext. Now, since everything in this "semi-functional" subgroup is randomized, the adversary cannot learn the appropriate structure that is being tested for by the decryption oracle. Hence, the only successful decryption queries it can produce must avoid this semi-functional space; we can use an adversary who produces such a query while receiving elements with random semi-functional components, however, to break a variant of subgroup decision. In this weak security game where no public parameters are given out, we can therefore prove IND-CCA1 security. Our notion of the weak game here is inspired by the new interpretation of dual system encryption techniques developed by Lewko and Waters [23].

To reduce full IND-CCA1 security to this weak version, we enlarge the space of our weakly secure scheme by adding two more subgroups so that we can project separately onto the components of the embedded scheme and the additional space; our construction then places meaningful components only in this additional space. To prove security, we first expand into the embedded space using a variant of subgroup decision. We now have a "shadow" copy of the scheme, attached to both keys and ciphertexts, that is not reflected in the public parameters, and we can project separately onto the real copy and onto this shadow copy. Thus, we can reduce full security to the weak security of the shadow scheme by having the reduction create the components in the real space itself and use projection to interpolate between an adversary on the full game and a challenger for the weak game.

4.1 An IBE with weak IND-CCA1 security

We first define a weak version of IND-CCA1 security for IBE, in which the adversary does not get to see the full public parameters, but only the bilinear group:

Definition 4.1. *For a bilinear group generator* $\mathsf{BilinearGen}$*, an IBE* $(\mathsf{Setup}, \mathsf{KeyExt}, \mathsf{Enc}, \mathsf{Dec})$*, an adversary* $\mathcal{A}$*, and a bit* b*, let* $p_b^{\mathcal{A}}(k)$ *be the probability of the event that* $b' = 0$ *in the following game:*

- *Step 1.* $\mathbb{G} \xleftarrow{\$} \mathsf{BilinearGen}(1^k)$*;* $(params, msk) \xleftarrow{\$} \mathsf{Setup}(\mathbb{G})$*.*
- *Step 2.* $(\mathsf{state}, m_0, m_1, id^*) \xleftarrow{\$} \mathcal{A}^{\mathsf{Dec}(params,msk,\cdot,\cdot),\mathsf{KeyExt}(params,msk,\cdot)}(\mathbb{G})$*.*

- *Step 3. If $|m_0| \neq |m_1|$ or $\mathcal{A}$ queried its* KeyExt *oracle on id^*, output $\perp$. Otherwise, output $c^* \xleftarrow{\$} \mathsf{Enc}(params, id^*, m_b)$.*
- *Step 4.* $b' \xleftarrow{\$} \mathcal{A}^{\mathsf{KeyExt}(params, msk, \cdot)}(\mathsf{state}, c^*)$.

We say that the IBE satisfies weak IND-CCA1 security *if for all PPT algorithms $\mathcal{A}$ there exists a negligible function $\nu(\cdot)$ such that $|p_0^{\mathcal{A}}(k) - p_1^{\mathcal{A}}(k)| < \nu(k)$.*

For our bilinear group, we require six subgroups on each side of the pairing; this means we run $\mathbb{G} = (N, G, H, G_T, e, \{g_i\}_i, \{h_i\}_i, \mu) \xleftarrow{\$} \mathsf{BilinearGen}(1^k, 6)$, where $G := \oplus_{i=1}^6 G_i = \langle g_i \rangle$, $H := \oplus_{i=1}^6 H_i = \langle h_i \rangle$, $e : G \times H \to G_T$, μ allows one to check membership in both G and H, and N is the maximum order of any element in these groups. We require that the message space is the cyclic subgroup generated by $e(g_1, h_1)$ in G_T. Our construction relies generically on the structure of the group and thus can be instantiated, as we see below, in either composite-order groups, using N as a product of distinct primes, or prime-order groups, using N as a prime. In addition to the regular canceling (and parameter hiding) requirements, we also require that specific generators $g_i \in G_i$ and $h_i \in H_i$ for all i, $1 \leq i \leq 4$, are chosen such that

$$e(g_1 g_2, h_1 h_2) = e(g_3 g_4, h_3 h_4) = 1. \tag{2}$$

Although this might seem like an additional requirement, as we see below and in Section 5, this property can be trivially constructed in prime-order and composite-order settings that satisfy the regular notion of canceling. This same sort of reorganization could also be applied to the original Boneh-Boyen construction by conceptualizing keys and ciphertexts as single elements in $G \times G$ instead of as pairs of elements in G, and more generally we consider the distinction between single group elements in a larger group and tuples of elements in a smaller group a matter of taste. (Of course, thinking of $G \times G$ as a single group results in certain cases of subgroup decision problems being easy, such as distinguishing $G \times 1_G$ from $G \times G$, but these cases will not come up.) Armed with such a bilinear group, we begin by presenting our IBE construction.

- $\mathsf{Setup}(\mathbb{G})$: Parse $\mathbb{G} = (N, G, H, G_T, e, \{g_i\}_{i=1}^6, \{h_i\}_{i=1}^6, \mu)$ and pick $\alpha \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$. Output $params := ((N, G, H, G_T, e, \mu), g_1, g_2, A := e(g_1, h_1)^\alpha)$ and $msk := (h_1^\alpha, \{h_i\}_{i=1}^6)$.
- $\mathsf{KeyExt}(params, msk, id)$: Pick $t, t', \gamma, \gamma', \beta, \beta' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and compute $sk_{id,1} := h_1^\alpha h_1^{tid} h_2^t h_5^\gamma h_6^\beta$ and $sk_{id,2} := h_1^{t' id} h_2^{t'} h_5^{\gamma'} h_6^{\beta'}$ Output $sk_{id} := (sk_{id,1}, sk_{id,2})$.
- $\mathsf{Enc}(params, id, M)$: Pick $s \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and compute $c_1 := M \cdot A^s$ and $c_2 := g_1^s \cdot g_2^{sid}$. Output $c := (c_1, c_2)$.
- $\mathsf{Dec}(params, sk_{id}, c)$: Check that $c_2 \in G$ and that $e(c_2, sk_{id,2}) = 1$; output $\perp$ if either of these does not pass. Otherwise, output $M := c_1 \cdot e(c_2, sk_{id,1})^{-1}$.

In addition, we note that msk can be used to decrypt directly; i.e., rather than form sk_{id} and decrypt in the usual way, we can instead compute $M = c_1 \cdot e(c_2, h_1^\alpha)^{-1}$.

Lemma 4.2. *If canceling and Equation 2 hold in $\mathbb{G}$, then the above construction describes a correct identity-based encryption scheme.*

Proof. To see that, for all identities id and messages M, $sk_{id} \xleftarrow{\$} \mathsf{KeyExt}(params, msk, id)$ correctly decrypts a ciphertext $c \xleftarrow{\$} \mathsf{Enc}(params, id, M)$, we first observe that the decryption check will pass, as

$$e(c_2, h_1^{t' id} h_2^{t'} h_5^{\gamma'} h_6^{\beta'}) = e(g_1^s \cdot g_2^{sid}, h_1^{id} h_2)^{t'} = e(g_1^s, h_1^{id})^{t'} \cdot e(g_2^{sid}, h_2)^{t'} = (e(g_1, h_1) e(g_2, h_2))^{st' id} = 1,$$

where the first equality follows from canceling and the last equality follows from Equation 2. Additionally, decryption succeeds in recovering the message, as

$$\begin{aligned} c_1 \cdot e\left(c_2, sk_{id,1}\right)^{-1} &= M \cdot A^s \cdot e(g_1^s g_2^{sid}, h_1^{\alpha} \cdot h_1^{tid} \cdot h_2^{t} \cdot h_5^{\gamma} \cdot h_6^{\beta})^{-1} \\ &= M \cdot e(g_1, h_1)^{\alpha s} \cdot e(g_1^s, h_1^{\alpha} \cdot h_1^{tid})^{-1} \cdot e(g_2^{sid}, h_2^{t})^{-1} \\ &= M \cdot e(g_1, h_1)^{\alpha s} \cdot e(g_1, h_1)^{-\alpha s} \cdot e(g_1, h_1)^{-stid} \cdot e(g_2, h_2)^{-stid} \\ &= M \cdot e(g_1, h_1)^{-stid} e(g_2, h_2)^{-stid} \\ &= M \cdot (e(g_1, h_1) e(g_2, h_2))^{-stid} \\ &= M, \end{aligned}$$

where the second equality again follows from canceling and the last from Equation 2. □

Theorem 4.3. *If canceling, parameter hiding, Equation 2, and generalized correlated subgroup decision hold in $\mathbb{G}$, then the above construction describes a weakly IND-CCA1-secure identity-based encryption scheme.*

To actualize these abstract requirements, for completeness we consider in Section 5 how they are satisfied in a composite-order bilinear group. In the prime-order setting, we already gave our augmented $\mathsf{BasicGen}$ construction in Section 3 (which we recall uses $n = 8$, $d = 1$, a scaling matrix C with all 1 entries, and auxiliary information μ that allows for a membership test in the first six subgroups), and proved that it satisfied canceling and parameter hiding, and that all nice instances of generalized correlated subgroup decision hold if SXDH holds. Our construction also uses $g_i = g^{\vec{v}_i}$ and $h_i = h^{-\vec{v}_i^*}$, so the definition of dual orthonormal bases ensures that Equation 2 holds as well. As all the instances we use in our proof are nice, we have the following corollary:

Corollary 4.4. *If SXDH holds in $\mathbb{G} \xleftarrow{\$} \mathsf{BasicGen}(1^k)$ and $\mathbb{G}$ uses augmented information μ, where $\mathsf{BasicGen}$ and augmented μ are as specified in Section 3, then the instantiation of the above construction in $\mathbb{G}$ is a weakly IND-CCA1-secure identity-based encryption scheme with identity space $\mathbb{F}_p$ and message space G_T.*

To prove Theorem 4.3, we proceed through a series of game transitions as follows; formal descriptions of the games and proofs of their indistinguishability can be found in Appendix A.

- Game_0. The honest weak IND-CCA1 game.
- Game_1. Switch to adding in a "duplicate" component in $G_3 \oplus G_4$ to the challenge ciphertext c_2^*; i.e., the value $g_3^{s'} g_4^{s' id}$. This is indistinguishable from Game_0 by subgroup decision.
- Game_2. Switch the $G_3 \oplus G_4$ component in c_2^* to be uniformly random. This is identical to Game_1 by parameter hiding.
- Game_3. Switch the keys returned by KeyExt to have random components in $H_3 \oplus H_4$ on $sk_{id,1}$ and on $sk_{id,2}$; i.e., values $h_3^{s'} h_4^{s''}$ (different values of s', s'' for $sk_{id,1}$ and $sk_{id,2}$). This is indistinguishable from Game_2 using a hybrid argument relying on subgroup decision and parameter hiding.
- Game_4. Switch from performing the decryption check with a term of the form $h_1^{t' id} h_2^{t'} h_5^{\gamma'} h_6^{\beta'}$ to using a term of the form $h_1^{t' id} h_2^{t'} h_3^{t'' id} h_4^{t''} h_5^{\gamma'} h_6^{\beta'}$. This is indistinguishable from Game_3 by subgroup decision.
- Game_5. Switch the Dec oracle to return $\perp$ on every query in which $c_2 \neq 1$, and 1 if $c_2 = 1$. This is indistinguishable from Game_4 by subgroup decision and parameter hiding.
- Game_6. Switch to encrypting a random message in the challenge ciphertext. This is indistinguishable from Game_5 by subgroup decision; furthermore, as there is now no information about the bit b, any adversary playing this game has advantage exactly zero.

4.2 Boosting to full IND-CCA1 security

With a weak IND-CCA1-secure IBE in place, we now consider how to augment it to achieve full IND-CCA1 security. Briefly, we do this by adding extra subgroups: to start, we assume we have a bilinear group $\widetilde{\mathbb{G}} := (N, \widetilde{G}, \widetilde{H}, \widetilde{G}_T, \widetilde{e}, \widetilde{\mu}) \xleftarrow{\$} \mathsf{BilinearGen}(1^k, 8)$; i.e., a group such that $\widetilde{G} := \oplus_{i=1}^{8} \widetilde{G}_i = \langle \widetilde{g}_i \rangle$, $\widetilde{H} := \oplus_{i=1}^{8} \widetilde{H}_i = \langle \widetilde{h}_i \rangle$, and $\widetilde{e} : \widetilde{G} \times \widetilde{H} \to \widetilde{G}_T$, and $\widetilde{\mu}$ allows one to efficiently test membership in $\widetilde{G}$ and $\widetilde{H}$. Once again, these subgroups should all be canceling, and satisfy

$$\widetilde{e}(\widetilde{g}_1\widetilde{g}_2, \widetilde{h}_1\widetilde{h}_2) = \widetilde{e}(\widetilde{g}_3\widetilde{g}_4, \widetilde{h}_3\widetilde{h}_4) = \widetilde{e}(\widetilde{g}_7\widetilde{g}_8, \widetilde{h}_7\widetilde{h}_8) = 1. \tag{3}$$

for a particular choice of generators $\widetilde{g}_i, \widetilde{h}_i$. Additionally, the group generation process should also produce a trapdoor τ that allows for the efficient computation of projection maps π_G and π_H such that $\pi_G : \widetilde{G} \to \widetilde{G}_1 \oplus \ldots \oplus \widetilde{G}_6$ and $\pi_H : \widetilde{H} \to \widetilde{H}_1 \oplus \ldots \oplus \widetilde{H}_6$; i.e., these map into subgroups analogous to the ones that we used in our construction of a weak IND-CCA1-secure IBE.

Finally, if we consider explicitly the group $\mathbb{G} = (N, \oplus_{i=1}^{6} G_i, \oplus_{i=1}^{6} H_i, G_T, e, \mu)$ from our weakly secure construction, then it should be the case that from $\mathbb{G}$ one can create $\widetilde{\mathbb{G}} := (N, \widetilde{G}, \widetilde{H}, \widetilde{G}_T, \widetilde{e}, \widetilde{\mu})$ such that $G_i = \widetilde{G}_i$ and $H_i = \widetilde{H}_i$ for all i, $1 \le i \le 6$, and τ can be derived from knowledge of μ. The message space and the space of possible identities are the same for the full scheme and the embedded weak scheme.

In our reduction to the weak IND-CCA1 security, we crucially rely on these projection maps, as well as one other property: if the groups $\widetilde{G}$ and $\widetilde{H}$ are generated from scratch, then generators for every subgroup will be known. If the groups are instead generated from the group description for the weak scheme, however, then not all such generators are known; we require that knowledge of suitable generators $\widetilde{g}_7$, $\widetilde{g}_8$, $\widetilde{h}_7$, and $\widetilde{h}_8$ be incorporated in τ, but the rest of the generators may be unknown.

We now give our construction in this framework:

- $\mathsf{Setup}(\widetilde{\mathbb{G}})$: Parse $\widetilde{\mathbb{G}} = (N, \widetilde{G}, \widetilde{H}, \widetilde{G}_T, \widetilde{e}, \widetilde{\mu}, \{\widetilde{g}_i\}_{i=1}^{8}, \{\widetilde{h}_i\}_{i=1}^{8})$ and pick $\alpha \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$. Output $params := (N, \widetilde{G}, \widetilde{H}, \widetilde{G}_T, \widetilde{e}, \widetilde{\mu}), \widetilde{g}_7, \widetilde{g}_8, A := \widetilde{e}(\widetilde{g}_7, \widetilde{h}_7)^{\alpha})$ and $msk := (\widetilde{h}_7^{\alpha}, \{\widetilde{h}_i\}_{i=1}^{8})$.
- $\mathsf{KeyExt}(params, msk, id)$: Pick $t, t', \gamma, \gamma', \delta, \delta' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and compute $sk_{id,1} := \widetilde{h}_7^{\alpha} \cdot \widetilde{h}_7^{tid} \cdot \widetilde{h}_8^{t} \cdot \widetilde{h}_5^{\gamma} \cdot \widetilde{h}_6^{\delta}$ and $sk_{id,2} := \widetilde{h}_7^{t'id} \cdot \widetilde{h}_8^{t'} \cdot \widetilde{h}_5^{\gamma'} \cdot \widetilde{h}_6^{\delta'}$. Output $sk_{id} := (sk_{id,1}, sk_{id,2})$.
- $\mathsf{Enc}(params, id, M)$: Pick $s \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and compute $c_1 := M \cdot A^s$, $c_2 := \widetilde{g}_7^{s} \cdot \widetilde{g}_8^{sid}$. Output $c := (c_1, c_2)$.
- $\mathsf{Dec}(params, sk_{id}, c)$: First check that $c_2 \in \widetilde{G}$ and that $\widetilde{e}(c_2, sk_{id,2}) = 1$; output $\perp$ if equality does not hold. Otherwise, output $M := c_1 \cdot \widetilde{e}(c_2, sk_{id,1})^{-1}$.

We note that decryption can again be simplified using msk; in this case, we compute $M = c_1 \cdot \widetilde{e}(c_2, \widetilde{h}_7^{\alpha})^{-1}$.

Lemma 4.5. *If canceling and Equation 3 hold in $\widetilde{\mathbb{G}}$, then the above construction describes a correct identity-based encryption scheme.*

Proof. To see that, for all identities id and messages M, $sk_{id} \xleftarrow{\$} \mathsf{KeyExt}(params, msk, id)$ correctly decrypts $c \xleftarrow{\$} \mathsf{Enc}(params, id, M)$, we first observe that the decryption check will pass, as $e(c_2, \widetilde{h}_5^{\gamma'}\widetilde{h}_6^{\delta'}) = 1$ by canceling, and

$$\widetilde{e}(c_2, \widetilde{h}_7^{t'id}\widetilde{h}_8^{t'}) = \widetilde{e}(\widetilde{g}_7^{s} \cdot \widetilde{g}_8^{sid}, \widetilde{h}_7^{t'id}\widetilde{h}_8^{t'}) = (\widetilde{e}(\widetilde{g}_7, \widetilde{h}_7)\widetilde{e}(\widetilde{g}_8, \widetilde{h}_8))^{st'id} = 1.$$

by canceling and Equation 3.

To additionally see that decryption will succeed in recovering the message, we have

$$\begin{aligned} c_1 \cdot \tilde{e}(c_2, sk_{id,1})^{-1} &= M \cdot A^s \cdot (\tilde{e}(\tilde{g}_7^s \cdot \tilde{g}_8^{sid}, \tilde{h}_7^\alpha \cdot \tilde{h}_7^{tid} \cdot \tilde{h}_8^t \cdot \tilde{h}_5^\gamma \cdot \tilde{h}_6^\beta)^{-1} \\ &= M \cdot \tilde{e}(\tilde{g}_7, \tilde{h}_7)^{\alpha s} \cdot \tilde{e}(\tilde{g}_7^s, \tilde{h}_7^\alpha \cdot \tilde{h}_7^{tid})^{-1} \cdot \tilde{e}(\tilde{g}_8^{sid}, \tilde{h}_8^t)^{-1} \\ &= M \cdot e(\tilde{g}_7, \tilde{h}_7)^{\alpha s} \cdot e(\tilde{g}_7, \tilde{h}_7)^{-\alpha s} \cdot e(\tilde{g}_7, \tilde{h}_7)^{-stid} \cdot e(\tilde{g}_8, \tilde{h}_8)^{-stid} \\ &= M \cdot (e(\tilde{g}_7, \tilde{h}_7) e(\tilde{g}_8, \tilde{h}_8))^{-stid} \\ &= M, \end{aligned}$$

where the second equality again follows from canceling and the last from Equation 3. □

Theorem 4.6. *If weak projecting, canceling, parameter hiding, Equation 3, and generalized correlated subgroup decision hold in $\tilde{\mathbb{G}}$, then the above construction is a IND-CCA1-secure identity-based encryption scheme.*

As we did for our weak IBE construction, we consider how to actualize these abstract requirements in both the composite-order and prime-order settings; for completeness, our composite-order construction and proofs that it satisfies these requirements can be found in Section 5. For the prime-order setting, we can now use our BasicGen construction from Section 3; here, as $\tilde{G} = G^8$, we can use our non-augmented construction, as testing membership in $\tilde{G}$ reduces to testing membership in G. We have already proved this setting satisfies weak projecting, canceling, and parameter hiding, and that the nice instances of generalized correlated subgroup decision hold if SXDH holds. As with our weak IBE, Equation 3 holds trivially by the definition of dual orthonormal bases.

We must also consider how to embed $\mathbb{G}$ into $\tilde{\mathbb{G}}$ as described above; this is also quite simple, however, as we can simply use $\tilde{G}_i = G_i$. The augmented auxiliary information μ for the weak scheme furthermore enables computation of the projection maps π_G and π_H, as knowledge of the spans of $\{\vec{v}_1, \ldots, \vec{v}_6\}$ and $\{\vec{v}_1^*, \ldots, \vec{v}_6^*\}$ allows one to compute a linear transformation that projects from $\mathbb{F}_p^8$ onto these spans, which can then be applied in the exponent to map onto $G_1 \oplus \ldots \oplus G_6$ and $H_1 \oplus \ldots \oplus H_6$.

As all of the instances of generalized correlated subgroup decision that we use in our proof of Theorem 4.6 are nice, we obtain the following corollary:

Corollary 4.7. *If SXDH holds in $\tilde{\mathbb{G}}$, where $\tilde{\mathbb{G}}$ is constructed from $\mathbb{G} \xleftarrow{\$} \mathsf{BasicGen}(1^k)$ as described above, then the instantiation of the above construction in $\tilde{\mathbb{G}}$ is an IND-CCA1-secure identity-based encryption scheme with identity space $\mathbb{F}_p$ and message space G_T.*

To prove Theorem 4.6, we proceed through the following series of game transitions:

- Game_0. The honest IND-CCA1 game.
- Game_1. Switch the secret keys returned by KeyExt to have additional "duplicate" elements in $\tilde{H}_1 \oplus \tilde{H}_2$ attached; i.e., elements of the form $\tilde{h}_1^\beta \tilde{h}_1^{t'id} \tilde{h}_2^{t'}$ on $sk_{id,1}$ and $\tilde{h}_1^{t''id} \tilde{h}_2^{t''}$ on $sk_{id,2}$. Switch Dec to use $\tilde{h}_1^\beta \tilde{h}_7^\alpha$ in place of just $\tilde{h}_7^\alpha$, and use a term of the form $\tilde{h}_1^{t''id} \tilde{h}_2^{t''} \tilde{h}_7^{tid} \tilde{h}_8^t \tilde{h}_5^{\gamma'} \tilde{h}_6^{\delta'}$ for the decryption check. This is indistinguishable from Game_0 by subgroup decision.
- Game_2. Switch the challenge ciphertext to add "duplicate" terms $\tilde{e}(\tilde{g}_1, \tilde{h}_1)^{\beta s'}$ to c_1^* and $\tilde{g}_1^{s'} \tilde{g}_2^{s'id}$ to c_2^*. This is indistinguishable from Game_1 by subgroup decision.

Finally, we show that if an adversary can win Game_2 then, using weak projection, it can be used to construct an adversary that breaks the weak IND-CCA1 security of the underlying scheme (i.e., the scheme constructed in the previous section). We therefore reduce the full IND-CCA1 security of this scheme to the weak IND-CCA1 security of the embedded scheme.

Following this outline, we begin by adding in extra components to secret keys, and changing decryption accordingly.

Game_0, $\boxed{\mathsf{Game}_1}$

$(N, \widetilde{G}, \widetilde{H}, \widetilde{G}_T, \widetilde{e}, \{\widetilde{g}_i\}_{i=1}^{8}, \{\widetilde{h}_i\}_{i=1}^{8}) \xleftarrow{\$} \mathsf{BilinearGen}(1^k, 8)$; $\widetilde{\mathbb{G}} \leftarrow (N, \widetilde{G}, \widetilde{H}, \widetilde{G}_T, \widetilde{e})$
$\alpha \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$, $\boxed{\alpha, \beta \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}}$; $A \leftarrow \widetilde{e}(\widetilde{g}_7, \widetilde{h}_7)^{\alpha}$, $msk \leftarrow \widetilde{h}_7^{\alpha}$, $\boxed{msk \leftarrow \widetilde{h}_1^{\beta}\widetilde{h}_7^{\alpha}}$
$params \leftarrow (\widetilde{\mathbb{G}}, \widetilde{g}_1, \widetilde{g}_2, \widetilde{h}_1, \widetilde{h}_2, A)$
$(\mathsf{state}, M_0, M_1, id^*) \xleftarrow{\$} \mathcal{A}^{\mathsf{KeyExt},\mathsf{Dec}}(\widetilde{\mathbb{G}})$
$b \xleftarrow{\$} \{0,1\}^*$
$s \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$; $c_1^* \leftarrow M_b \cdot A^s$, $c_2^* \leftarrow \widetilde{g}_7^{s} \cdot \widetilde{g}_8^{s id^*}$
$b' \xleftarrow{\$} \mathcal{A}^{\mathsf{KeyExt}}(\mathsf{state}, (c_1^*, c_2^*))$

Procedure $\mathsf{KeyExt}(id)$

$t, t', \gamma, \gamma', \delta, \delta' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$, $\boxed{t, t', t'', t''', \gamma, \delta, \gamma', \delta' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}}$
return $sk_{id}^1 := \widetilde{h}_7^{\alpha} \cdot \widetilde{h}_7^{tid} \cdot \widetilde{h}_8^{t} \cdot \widetilde{h}_5^{\gamma} \cdot \widetilde{h}_6^{\delta}$, $sk_{id}^2 := \widetilde{h}_7^{t'id} \cdot \widetilde{h}_8^{t'} \cdot \widetilde{h}_5^{\gamma'} \cdot \widetilde{h}_6^{\delta'}$
$\boxed{\text{return } sk_{id,1} := \widetilde{h}_1^{\beta}\widetilde{h}_1^{t''id}\widetilde{h}_2^{t''} \cdot \widetilde{h}_7^{\alpha}\widetilde{h}_7^{tid} \cdot \widetilde{h}_8^{t} \cdot \widetilde{h}_5^{\gamma} \cdot \widetilde{h}_6^{\delta},\ sk_{id,2} := \widetilde{h}_1^{t'''id}\widetilde{h}_2^{t'''}\widetilde{h}_7^{t'id} \cdot \widetilde{h}_8^{t'} \cdot \widetilde{h}_5^{\gamma'} \cdot \widetilde{h}_6^{\delta'}}$

Procedure $\mathsf{Dec}(id, (c_1, c_2))$

$t, \gamma, \delta \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$, $\boxed{t, t', \gamma, \delta \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}}$
if $\widetilde{e}(c_2, \widetilde{h}_7^{tid}\widetilde{h}_8^{t}h_5^{\gamma}h_6^{\delta}) \neq 1$ return $\perp$ $\boxed{\text{if } \widetilde{e}(c_2, \widetilde{h}_1^{t'id}\widetilde{h}_2^{t'}\widetilde{h}_7^{tid}\widetilde{h}_8^{t}h_5^{\gamma}h_6^{\delta}) \neq 1 \text{ return } \perp}$
return $c_1 \cdot \widetilde{e}(c_2, msk)^{-1}$

Lemma 4.8. *If the generalized correlated subgroup decision assumption holds, then* Game_0 *is computationally indistinguishable from* Game_1.

Proof. We assume there exists an adversary $\mathcal{A}$ that can distinguish between Game_0 and Game_1 with some non-negligible advantage and use it to construct an adversary $\mathcal{B}$ that solves an instance of the generalized correlated subgroup decision problem with related non-negligible advantage. We invoke the instance of the assumption parameterized by sets $S_G := \{7, 8\}$, $S_H := \{3, 4, 5, 6, 7, 8\}$, $T_1 = \{(7, 8)\}$, and $T_2 = \{(1, 2), (7, 8)\}$, with challenge terms in $\widetilde{H}$.

$\mathcal{B}$ receives as input $\widetilde{\mathbb{G}} = (N, \widetilde{G}, \widetilde{H}, \widetilde{G}_T, \widetilde{e})$ and elements

$$(\widetilde{g}_7, \widetilde{g}_8, \widetilde{h}_3, \ldots, \widetilde{h}_8, T, T'),$$

where either $(T, T') = (\widetilde{h}_7^{v}, \widetilde{h}_8^{v})$ or $(T, T') = (\widetilde{h}_7^{v}\widetilde{h}_1^{z}, \widetilde{h}_8^{v}\widetilde{h}_2^{z})$ for $v, z \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$. $\mathcal{B}$ implicitly sets $\alpha = v$ and gives $params := (\widetilde{\mathbb{G}}, \widetilde{g}_7, \widetilde{g}_8, \widetilde{e}(\widetilde{g}_7, T))$ to $\mathcal{A}$.

On KeyExt queries for an identity id, $\mathcal{B}$ picks random $t, t', \delta, \delta', \sigma, \sigma', \eta, \eta' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and returns

$$sk_{id,1} := T \cdot T^{\eta id} \cdot (T')^{\eta}\widetilde{h}_7^{tid}\widetilde{h}_8^{t}\widetilde{h}_5^{\delta}\widetilde{h}_6^{\sigma},\ sk_{id,2} := T^{\eta' id} \cdot (T')^{\eta'}\widetilde{h}_7^{t'id}\widetilde{h}_8^{t'}\widetilde{h}_5^{\delta'}\widetilde{h}_6^{\sigma'},$$

Note that if $(T, T') = (\widetilde{h}_7^{v}, \widetilde{h}_8^{v})$, this is distributed as in Game_0. If instead $(T, T') = (\widetilde{h}_7^{v}\widetilde{h}_1^{z}, \widetilde{h}_8^{v}\widetilde{h}_2^{z})$, then this is distributed as in Game_1, with $\beta := z$.

On Dec queries for $(id, (c_1, c_2))$, $\mathcal{B}$ picks random values $t', \delta', \sigma', \eta' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and checks that $\widetilde{e}(c_2, T^{\eta' id} \cdot (T')^{\eta'}\widetilde{h}_7^{t'id}\widetilde{h}_8^{t'}\widetilde{h}_5^{\delta'}\widetilde{h}_6^{\sigma'}) = 1$ and outputs $\perp$ if this check fails. Otherwise, it returns

$$M := c_1 \cdot \widetilde{e}(c_2, T\widetilde{h}_7^{id}\widetilde{h}_8)^{-1}.$$

Note that if $T = \widetilde{h}_7^{v}$, this will produce the same responses as the decryption oracle in Game_0, and if $T = \widetilde{h}_7^{v}\widetilde{h}_1^{z}$, this will produce the same responses as the decryption oracle in Game_1.

Since $\mathcal{B}$ knows the public parameters, it can simply use the regular encryption algorithm to produce the challenge ciphertext. It can therefore leverage $\mathcal{A}$'s non-negligible advantage in distinguishing between Game_0 and Game_1 to achieve a non-negligible advantage against this instance of the correlated subgroup decision problem. $\square$

Next, in Game_2, we add in duplicate components to the challenge ciphertext as well. This means changing Game_1 as follows:

$$\mathsf{Game}_1, \boxed{\mathsf{Game}_2}$$

$$6 \quad s \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}, \boxed{s, s' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}}; c_1^* \leftarrow M_b \cdot A^s, \boxed{c_1^* \leftarrow M_b \cdot A^s \cdot \widetilde{e}(\widetilde{g}_1, \widetilde{h}_1)^{\beta s'}},$$
$$c_2^* \leftarrow \widetilde{g}_7^s \cdot \widetilde{g}_8^{s id^*}, \boxed{c_2^* \leftarrow \widetilde{g}_7^s \cdot \widetilde{g}_8^{s id^*} \cdot \widetilde{g}_1^{s'} \cdot \widetilde{g}_2^{s' id^*}}$$

Lemma 4.9. *If the generalized correlated subgroup decision assumption holds, then* Game_1 *is computationally indistinguishable from* Game_2*.*

Proof. We assume there exists an adversary $\mathcal{A}$ that can distinguish between Game_1 and Game_2 with some non-negligible advantage and use it to construct an adversary $\mathcal{B}$ that solves an instance of the generalized correlated subgroup decision problem with related non-negligible advantage. We invoke the instance of the assumption parameterized by sets $S_G := \{7, 8\}$, $S_H := \{3, 4, 5, 6, 7, 8, ((1, 2), (7, 8))\}$, $T_1 = \{(7, 8)\}$, and $T_2 = \{(1, 2), (7, 8)\}$, with challenge terms in $\widetilde{G}$.

To start, $\mathcal{B}$ receives as input $\widetilde{\mathbb{G}} = (N, \widetilde{G}, \widetilde{H}, \widetilde{G}_T, \widetilde{e})$ and elements

$$(\widetilde{g}_7, \widetilde{g}_8, \widetilde{h}_3, \ldots, \widetilde{h}_8, \widetilde{h}_{1,7} := \widetilde{h}_1^z \widetilde{h}_7^t, \widetilde{h}_{2,8} := \widetilde{h}_2^z \widetilde{h}_8^t, T, T'),$$

where either $(T, T') = (\widetilde{g}_7^s, \widetilde{g}_8^s)$ or $(T, T') = (\widetilde{g}_7^s \widetilde{g}_1^w, \widetilde{g}_8^s \widetilde{g}_2^w)$ for $z, t, s, w \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$. $\mathcal{B}$ then picks a random $\alpha' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and implicitly sets $\alpha := t\alpha'$ and $\beta := z\alpha'$. It then gives $params := (\widetilde{\mathbb{G}}, \widetilde{g}_7, \widetilde{g}_8, \widetilde{e}(\widetilde{g}_7, \widetilde{h}_{1,7})^{\alpha'})$ to $\mathcal{A}$.

On KeyExt queries for an identity id, $\mathcal{B}$ chooses random $\delta, \delta', \sigma, \sigma', \eta, \eta', \gamma, \gamma' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and returns

$$sk_{id}^1 := \widetilde{h}_{1,7}^{\alpha'} \widetilde{h}_{1,7}^{\eta id} \widetilde{h}_{2,8}^{\eta} \widetilde{h}_7^{\gamma id} \widetilde{h}_8^{\gamma} \widetilde{h}_5^{\delta} \widetilde{h}_6^{\sigma} = \widetilde{h}_1^{z\alpha'} \widetilde{h}_1^{z\eta id} \cdot \widetilde{h}_7^{t\alpha'} \widetilde{h}_7^{t\eta id} \cdot \widetilde{h}_2^{z\eta} \cdot \widetilde{h}_7^{\gamma id} \cdot \widetilde{h}_8^{t\eta} \widetilde{h}_8^{\gamma} \cdot \widetilde{h}_5^{\delta} \cdot \widetilde{h}_6^{\sigma},$$

$$sk_{id}^2 := \widetilde{h}_{1,7}^{\eta' id} \widetilde{h}_{2,8}^{\eta'} \widetilde{h}_7^{\gamma' id} \widetilde{h}_8^{\gamma'} \widetilde{h}_5^{\delta'} \widetilde{h}_6^{\sigma'} = \widetilde{h}_1^{z\eta' id} \cdot \widetilde{h}_7^{t\eta' id} \cdot \widetilde{h}_2^{z\eta'} \cdot \widetilde{h}_7^{\gamma' id} \cdot \widetilde{h}_8^{t\eta'} \widetilde{h}_8^{\gamma'} \cdot \widetilde{h}_5^{\delta'} \cdot \widetilde{h}_6^{\sigma'},$$

which, for $\beta := z\alpha'$, is distributed identically to the key computed in both Game_1 and Game_2.

On Dec queries of the form $(id, (c_1, c_2))$, $\mathcal{B}$ chooses random $\eta', \gamma', \delta', \sigma' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and checks that $\widetilde{e}(c_2, \widetilde{h}_{1,7}^{\eta' id} \widetilde{h}_{2,8}^{\eta'} \widetilde{h}_7^{\gamma' id} \widetilde{h}_8^{\gamma'} \widetilde{h}_5^{\delta'} \widetilde{h}_6^{\sigma'}) = 1$, and outputs $\perp$ if any of this check fails. Otherwise, it returns

$$M := c_1 \cdot \widetilde{e}(c_2, \widetilde{h}_{1,7}^{\alpha'} \widetilde{h}_7^{id} \widetilde{h}_8)^{-1}.$$

To produce the challenge ciphertext for id^*, $\mathcal{B}$ picks $b \xleftarrow{\$} \{0, 1\}$ and computes

$$c_1 := M_b \widetilde{e}(T, \widetilde{h}_{1,7}^{\alpha'}) \quad \text{and} \quad c_2 := T(T')^{id^*}.$$

If $(T, T') = (\widetilde{g}_7^s, \widetilde{g}_8^s)$, this is a properly distributed encryption of M_b for Game_1. If instead $(T, T') = (\widetilde{g}_7^s \widetilde{g}_1^w, \widetilde{g}_8^s \widetilde{g}_2^w)$, this is a properly distributed encryption of M_b for Game_2 (with $s' = w$). Thus, $\mathcal{B}$ can leverage $\mathcal{A}$'s non-negligible difference in advantage between these games to achieve a non-negligible advantage against this instance of the generalized correlated subgroup decision problem. $\square$

Lemma 4.10. *If the embedded scheme is weakly IND-CCA1 secure and weak projecting holds in* $\widetilde{\mathbb{G}}$*, then no PPT adversary can achieve a non-negligible advantage in* Game_2*.*

Proof. We assume there exists an adversary $\mathcal{A}$ that achieves a non-negligible advantage in Game_2, and use it to construct an adversary $\mathcal{B}$ that has related non-negligible advantage in the weak IND-CCA1 game for the embedded scheme. To start, $\mathcal{B}$ receives as input $\mathbb{G} = (N, G, H, G_T, e, \mu)$. It then constructs $\widetilde{\mathbb{G}} = (N, \widetilde{G}, \widetilde{H}, \widetilde{G}_T, \widetilde{e}, \widetilde{\mu})$ with the properties described above; as a reminder, this is done in such a way that $\mathcal{B}$ knows the trapdoor information τ and suitable generators $\widetilde{g}_7$, $\widetilde{g}_8$, $\widetilde{h}_7$, and $\widetilde{h}_8$. It then picks $\alpha \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$, and gives $params := (\widetilde{\mathbb{G}}, \widetilde{g}_7, \widetilde{g}_8, \widetilde{e}(\widetilde{g}_7, \widetilde{h}_7)^\alpha)$ to $\mathcal{A}$.

On KeyExt queries for an identity id, $\mathcal{B}$ first outputs id as its own KeyExt query to receive back $sk_{id,1}, sk_{id,2} \in H_1 \oplus H_2 \oplus H_5 \oplus H_6$. It then chooses $t, t' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and computes its response as

$$((sk_{id,1})' := \widetilde{h}_7^\alpha \cdot \widetilde{h}_7^{tid} \cdot \widetilde{h}_8^t \cdot sk_{id,1}, (sk_{id,2})' := \widetilde{h}_7^{t'id} \cdot \widetilde{h}_8^{t'} \cdot sk_{id,2}).$$

We note that this produces properly distributed keys.

On Dec queries of the form $(id, (c_1, c_2))$, $\mathcal{B}$ first chooses a random $t \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and checks if $\widetilde{e}(c_2, h_7^{tid} h_8^t) = 1$. If this check fails, it outputs $\perp$. (Since t is randomly chosen, there is only a negligible chance that $\mathcal{A}$ can produce a query that fails this check but pass the decryption check with the additional terms in $\widetilde{H}$ present.) Otherwise, it outputs its own Dec query

$$(id, 1, \pi_G(c_2)),$$

where here 1 denotes the identity element in G_T. If it receives $\perp$ in response, it replies with $\perp$ to $\mathcal{A}$. If instead it receives some $X \in G_T$, it returns to $\mathcal{A}$ the message

$$M := c_1 \cdot X \cdot \left(\widetilde{e}(c_2, \widetilde{h}_7^\alpha \widetilde{h}_7^{id} \widetilde{h}_8)\right)^{-1}.$$

To see that this properly simulates the decryption oracle, note that when the decryption checks pass, we have

$$\mathsf{Dec}(sk, (c_1, c_2)) = c_1 \cdot \widetilde{e}(c_2, (sk_{id,1})')^{-1} = c_1 \cdot \widetilde{e}(c_2, sk_{id,1})^{-1} \cdot \left(\widetilde{e}(c_2, \widetilde{h}_7^\alpha \widetilde{h}_7^{id} \widetilde{h}_8)\right)^{-1}.$$

Moreover, we have

$$\widetilde{e}(c_2, sk_{id,1})^{-1} = e(\pi_G(c_2), sk_{id,1})^{-1} = X$$

(by construction of the decryption algorithm for the embedded weakly secure scheme).

Finally, when $\mathcal{A}$ outputs its challenge (M_0, M_1, id^*), $\mathcal{B}$ outputs M_0, M_1, id^* as its own challenge to receive back a ciphertext (c_1', c_2'). It then picks $s \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and computes

$$c_1^* := c_1' \cdot \widetilde{e}(\widetilde{g}_7, \widetilde{h}_7)^{\alpha s} \quad \text{and} \quad c_2^* := c_2' \cdot \widetilde{g}_7^s \cdot \widetilde{g}_8^{sid},$$

and gives (c_1, c_2) as the challenge ciphertext to $\mathcal{A}$. We note that this is a properly distributed ciphertext. When $\mathcal{A}$ outputs its guess bit b', $\mathcal{B}$ outputs the same bit. □

5 A Composite-Order Instantiation of Our IBE

To show that we can instantiate our IBE constructed in Section 4 (both the weakly and fully IND-CCA1 variants), we must construct a composite-order bilinear group that satisfies weak projecting, canceling, parameter hiding, and generalized correlated subgroup decision.

We begin with a symmetric bilinear group (N, G', G_T', e'), where $N = pqrs$ for distinct primes p, q, r, and s, and $G' = G_p \oplus G_q \oplus G_r \oplus G_s$ for $G_p = \langle g_p \rangle$, $G_q = \langle g_q \rangle$, $G_r = \langle g_r \rangle$, and $G_s = \langle g_s \rangle$. The first three primes are used in our weak scheme, and the last prime s is used to embed the weak scheme into the full scheme.

We then pick random values $a, b \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and define $G := G_1 \oplus \ldots \oplus G_6$ to be $G_pG_qG_r \times G_pG_qG_r$, where $G_1 := \langle(g_p, g_p^a)\rangle$, $G_2 := \langle(1, g_p^b)\rangle$, $G_3 := \langle(g_q, g_q^a)\rangle$, $G_4 := \langle(1, g_q^b)\rangle$, $G_5 := \langle(g_r, 1)\rangle$, and $G_6 := \langle(1, g_r)\rangle$. To provide a membership test for G, we assume that we are given the prime s as part of μ, so pqr and s are separately known, but it is still hard to factor pqr.

Similarly, we define $H = H_1 \oplus \ldots \oplus H_6$ to be $G_pG_qG_r \times G_pG_qG_r$, where $H_1 := \langle(g_p^b, 1)\rangle$, $H_2 := \langle(g_p^a, g_p^{-1})\rangle$, $H_3 := \langle(g_q^b, 1)\rangle$, $H_4 := \langle(g_q^a, g_q^{-1})\rangle$, $H_5 := \langle(g_r, 1)\rangle$, and $H_6 := \langle(1, g_r)\rangle$. We define $e : G \times H \to G_T$ by

$$e((g, g'), (h, h')) := e'(g, h) \cdot e'(g', h') \; \forall g, g', h, h' \in G',$$

and set $\mathbb{G} = (N, G, H, G_T := G'_T, e, \mu)$. It is easy to verify that e satisfies both bilinearity and non-degeneracy. In addition, as pairing elements in any of the two subgroups (e.g., G_p and G_q) yields the identity, a case-by-case analysis reveals that canceling is satisfied as well; for example, to show that $e(G_1, H_3) = 1$, we observe that, to have order p, we must have $g_p = (g')^{\alpha qrs}$ for some $\alpha \in \mathbb{Z}/N\mathbb{Z}$, and similarly have $g_q = (g')^{\beta prs}$ for some $\beta \in \mathbb{Z}/N\mathbb{Z}$, where g' is a generator of G'. We therefore have

$$e((g_p, g_p^a), (g_q^b, 1)) = e'(g_p, g_q^b) \cdot e'(g_p^a, 1) = e((g')^{\alpha qrs}, (g')^{b\beta prs}) = e(g', g')^{b\alpha\beta pqr^2 s^2} = e(g', g')^{b\alpha\beta rs \cdot N} = 1.$$

Projecting is also satisfied, as the Chinese Remainder theorem implies that we can efficiently construct, for example, a value λ_p such that

$$\lambda_p \equiv \begin{cases} 1 \bmod p \\ 0 \bmod q \\ 0 \bmod r, \end{cases}$$

and thus project G' into G_p and, incorporating the values a and b as well, into the subgroups G_i and H_i accordingly. Finally, Equation 2 is satisfied, as

$$e(g_1 g_2, h_1 h_2) = e'(g_p, g_p^b) \cdot e'(g_p^b, g_p^{-1}) = 1,$$

and

$$e(g_3 g_4, h_3 h_4) = e'(g_q, g_q^a) \cdot e'(g_q^a, g_q^{-1}) = 1,$$

so that $e(g_1 g_2, h_1 h_2) = e(g_3 g_4, h_3 h_4) = 1$ as required.

We note that the message space for the scheme will be the subgroup of G_T of order p. This is not the usual case, as messages are typically be assumed to come from the larger group G_T. However, this strange feature is circumvented in the prime-order case, where we can adjust things to work with the typical message space of G_T. We view this composite-order construction mostly as an instructive demonstration of our proof techniques rather than as a scheme recommended for practice, so we are not overly concerned with the oddity of the message space here.

We show that parameter hiding is satisfied as well in the following lemma:

Lemma 5.1. *The parameter hiding requirement in Example 2.7 holds for $\mathbb{G} = (N, G, H, G_T, e, \mu)$ defined as above.*

Proof. To prove that the distributions in Example 2.7 are equivalent, we observe that $h_3^{zy} h_4^z = (g_q^{bzy} \cdot g_q^{az}, g_q^{-z}) = (g_q^{z(a+by)}, g_q^{-z})$ and $g_3^w g_4^{wx} = (g_q^w, g_q^{aw} \cdot g_q^{bwx}) = (g_q^w, g_q^{w(a+bx)})$. By the Chinese Remainder Theorem, the values of a, b modulo q are uniformly random and independent of their values modulo the other primes. Thus, when $x \neq y$, the values $ax + b$ and $ay + b$ are distributed uniformly at random modulo q, since $f(\phi) = a\phi + b$ is a pairwise independent function modulo q. □

All it remains to show is that generalized correlated subgroup decision holds in this setting. To do this, we use the generalized subgroup decision assumption, formalized by Bellare et al. [4]. Our formalization also allows for a single prime s to be revealed, and requires subgroup decision hardness only within the subgroups of the other prime orders. We state this as follows:

Assumption 5.2. **[18]** *Let* $(S_0, S_1, \ldots, S_k)$ *be non-empty subsets of* $[m]$ *such that for each* $2 \le j \le k$*, either* $S_j \cap S_0 = \emptyset = S_j \cap S_1$ *or* $S_j \cap S_0 \neq \emptyset \neq S_j \cap S_1$*. Given a bilinear group generator* BilinearGen*, define the following distribution:*

$$\mathbb{G} = (N = p_1 \ldots p_m p_{m+1}, p_{m+1}, G, G_T, e) \xleftarrow{\$} \mathsf{BilinearGen}(1^k),$$
$$Z_0 \xleftarrow{\$} G_{S_0}, Z_1 \xleftarrow{\$} G_{S_1}, \ \ldots, \ Z_k \xleftarrow{\$} G_{S_k},$$
$$D := (\mathbb{G}, Z_2, \ldots, Z_k).$$

(Here, the notation G_{S_i} *denotes the subgroup of order* $\prod_{j \in S_i} p_j$*.) Then for any PPT algorithm* $\mathcal{A}$ *there exists a negligible function* $\nu(\cdot)$ *such that*

$$|Pr[\mathcal{A}(D, Z_0) = 1] - Pr[\mathcal{A}(D, Z_1) = 1]| < \nu(k).$$

Lemma 5.3. *If the generalized subgroup decision assumption holds in* $\mathbb{G}$*, so does generalized correlated subgroup decision.*

Proof. We consider an arbitrary instance of generalized correlated subgroup decision described by sets S_G, S_H, T_1, and T_2; without loss of generality we assume the challenge terms are in G. We associate the pair $(1, 2)$ with the prime p, the pair $(3, 4)$ with the prime q, and the pair $(5, 6)$ with the prime r. In this way, we can re-interpret T_1 and T_2 as subsets of $\{p, q, r\}$ that differ in precisely one element. We then consider an instance of the generalized subgroup decision assumption for the composite-order group G' where the challenge term is either a random element of the subgroup whose order is the product of the primes in T_1 or a random element of the subgroup whose order is the product of the primes in T_2. We may assume that generators of all prime-order subgroups are given out *except* for the prime that differs between T_1 and T_2. Also, for any subset Z of $\{p, q, r\}$ such that $T_1 \cap Z \neq \emptyset \neq T_2 \cap Z$, we may assume that a random element is given out from the subgroup whose order is the product of the primes in Z.

We now observe that such elements must suffice to produce the elements of G and H prescribed by S. We choose $a, b \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and can then produce all of the required generators, since S cannot include single numbers corresponding to the prime that differentiates between T_1 and T_2. Now, any tuple of pairs that appears in S and involves the prime for which we are not given a generator must also include a pair that is common to T_1 and T_2. Hence, we have been given a random element X from the subgroup whose order is the product of the primes corresponding to the pairs in the tuple. To produce the correlated samples, we simply choose a random exponent $t \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and take X raised to appropriate powers in terms of a and b. For example, suppose that X is a random element of $G_p G_q$, and we are tasked with creating correlated samples from $G_1 \oplus G_3$ and $G_2 \oplus G_4$; then we produce (X, X^{ta}) and $(1, X^{tb})$. The fact that this is properly distributed as a correlated sample follows from the Chinese Remainder theorem, as the values of t modulo p and q are independent and each uniformly random. □

By construction, we have now proved the following theorem:

Theorem 5.4. *If generalized subgroup decision holds in* $\mathbb{G}$ *as described above, then the instantiation of the construction in Section 4.1 in* $\mathbb{G}$ *is a weakly IND-CCA1-secure identity-based encryption scheme.*

We would also like to prove the corresponding theorem for the fully secure variant. To do this, we need to show that a group G of order $N = pqrs$ can be constructed using the previously defined group G' of order pqr. We observe that we could treat G' as a subgroup of this larger group $G = G' \oplus G_s$, and restrict ourselves to computations within this subgroup, letting a generator g_s for this additional subgroup be known. (While this process of restricting computation to strictly within G' might reveal s, we allow s to be known anyway.) We assume that this process of thus "embedding" a group of order

pqr into a group G of order $pqrs$ for known s generates the trapdoor knowledge τ that allows one to efficiently compute projection maps from G into G'.

We then define $\widetilde{G} := \widetilde{G}_1 \oplus \ldots \oplus \widetilde{G}_8 = G^2$, with the generators $\widetilde{g}_1, \ldots, \widetilde{g}_6$ and $\widetilde{h}_1, \ldots, \widetilde{h}_6$ defined as before, and the additional generators defined as $\widetilde{g}_7 := (g_s, g_s^{a'})$, $\widetilde{g}_8 := (1, g_s^{b'})$ $\widetilde{h}_7 := (g_s^{b'}, 1)$, and $\widetilde{h}_8 := (g_s^{a'}, g_s^{-1})$ for $a', b' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$, where $N = pqrs$. We define $\widetilde{e}$ by

$$\widetilde{e}((g, g'), (h, h')) := e'(g, h) \cdot e'(g', h') \ \forall g, g', h, h' \in G,$$

and thus use $\widetilde{G}_T := G'_T$. Finally, knowledge of s allows one to project onto G_{pqr} and H_{pqr}, and the correlated subgroup decision assumption for this expanded setting follows from the generalized subgroup decision assumption for G of order $N = pqrs$ by the same argument applied above for the case of three primes, which proves the following theorem:

Theorem 5.5. *If generalized subgroup decision holds in $\widetilde{\mathbb{G}}$, then the instantiation of the construction in Section 4.2 in $\widetilde{\mathbb{G}}$ is an IND-CCA1-secure identity-based encryption scheme.*

References

[1] D. Aranha, J.-L. Beuchat, J. Detrey, and N. Estibals. Optimal eta pairing on supersingular genus-2 binary hyperelliptic curves. In *Proceedings of CT-RSA 2012*, pages 98–115, 2012.

[2] D. Aranha, K. Karabina, P. Longa, C. Geboyts, and J. López. Faster explicit formulas for computing pairings over ordinary curves. In *Proceedings of Eurocrypt 2011*, pages 48–68, 2011.

[3] L. Ballard, M. Green, B. de Medeiros, and F. Monrose. Correlation-resistant storage via keyword-searchable encryption. Cryptology ePrint Archive, Report 2005/417, 2005. `http://eprint.iacr.org/`.

[4] M. Bellare, B. Waters, and S. Yilek. Identity-based encryption secure against selective opening attack. In *Proceedings of TCC 2011*, pages 235–252, 2011.

[5] D. Boneh and X. Boyen. Efficient selective-ID security identity based encryption without random oracles. In *Proceedings of Eurocrypt 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 223–238. Springer-Verlag, 2004.

[6] D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In *Proceedings of Crypto 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 41–55. Springer-Verlag, 2004.

[7] D. Boneh, E.-J. Goh, and K. Nissim. Evaluating 2-DNF formulas on ciphertexts. In *Proceedings of the 2nd Theory of Cryptography Conference (TCC)*, volume 3378 of *Lecture Notes in Computer Science*, pages 325–341. Springer-Verlag, 2005.

[8] D. Boneh, K. Rubin, and A. Silverberg. Finding ordinary composite order elliptic curves using the Cocks-Pinch method. *Journal of Number Theory*, 131(5):832–841, 2011.

[9] X. Boyen and B. Waters. Compact group signatures without random oracles. In *Proceedings of Eurocrypt 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 427–444. Springer-Verlag, 2006.

[10] X. Boyen and B. Waters. Full-domain subgroup hiding and constant-size group signatures. In *Proceedings of PKC 2007*, volume 4450 of *Lecture Notes in Computer Science*, pages 1–15. Springer-Verlag, 2007.

[11] R. Canetti, S. Halevi, and J. Katz. A forward-secure public-key encryption scheme. In *Proceedings of Eurocrypt 2003*, pages 255–271, 2003.

[12] J. Chen, H. W. Lim, S. Ling, H. Wang, and H. Wee. Shorter IBE and signatures via asymmetric pairings. In *Proceedings of Pairing 2012*, 2012.

[13] D. M. Freeman. Converting pairing-based cryptosystems from composite-order groups to prime-order groups. In *Proceedings of Eurocrypt 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 44–61. Springer-Verlag, 2010.

[14] S. Galbraith, K. Paterson, and N. Smart. Pairings for cryptographers. *Discrete Applied Mathematics*, 156(16):3113–21, 2008.

[15] A. Guillevic. Comparing the pairing efficiency over composite-order and prime-order elliptic curves. In *Proceedings of ACNS 2013*, 2013. To appear.

[16] T. Hayashi, T. Shimoyama, N. Shinohara, and T. Takagi. Breaking pairing-based cryptosystems using η_t pairing over $GF(3^{97})$. Cryptology ePrint Archive, Report 2012/345, 2012. http://eprint.iacr.org/2012/345.

[17] J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In *Proceedings of Eurocrypt 2008*, volume 4965 of *Lecture Notes in Computer Science*, pages 146–162. Springer-Verlag, 2008.

[18] A. Lewko. Tools for simulating features of composite order bilinear groups in the prime order setting. In *Proceedings of Eurocrypt 2012*, pages 318–335, 2012.

[19] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner production encryption. In *Proceedings of Eurocrypt 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 62–91. Springer-Verlag, 2010.

[20] A. Lewko and B. Waters. New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In *Proceedings of the 7th Theory of Cryptography Conference (TCC)*, volume 5978 of *Lecture Notes in Computer Science*, pages 455–479. Springer-Verlag, 2010.

[21] A. Lewko and B. Waters. Decentralizing attribute-based encryption. In *Proceedings of Eurocrypt 2011*, volume 6632 of *Lecture Notes in Computer Science*, pages 568–588. Springer-Verlag, 2011.

[22] A. Lewko and B. Waters. Unbounded HIBE and attribute-based encryption. In *Proceedings of Eurocrypt 2011*, volume 6632 of *Lecture Notes in Computer Science*, pages 547–567. Springer-Verlag, 2011.

[23] A. Lewko and B. Waters. New proof methods for attribute-based encryption: Achieving full security through selective techniques. In *Proceedings of Crypto 2012*, pages 180–198, 2012.

[24] S. Meiklejohn, H. Shacham, and D. M. Freeman. Limitations on transformations from composite-order to prime-order groups: the case of round-optimal blind signatures. In *Proceedings of Asiacrypt 2010*, pages 519–538, 2010.

[25] T. Okamoto and K. Takashima. Homomorphic encryption and signatures from vector decomposition. In *Proceedings of Pairing 2008*, pages 57–74, 2008.

[26] T. Okamoto and K. Takashima. Hierarchical predicate encryption for inner-products. In *Proceedings of Asiacrypt 2009*, pages 214–231, 2009.

[27] T. Okamoto and K. Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In *Proceedings of Crypto 2010*, pages 191–208, 2010.

[28] M. Scott. On the efficient implementation of pairing-based protocols. In *Proceedings of IMACC 2011*, pages 296–308, 2011.

[29] J. H. Seo. On the (im)possibility of projecting property in prime-order setting. In *Proceedings of Asiacrypt 2012*, pages 61–79, 2012.

[30] J. H. Seo and J. H. Cheon. Beyond the limitation of prime-order groups, and round optimal blind signatures. In *Proceedings of TCC 2012*, volume 7194 of *Lecture Notes in Computer Science*, pages 133–150, 2012.

[31] B. Waters. Dual system encryption: Realizing fully secure ibe and hibe under simple assumptions. In *Proceedings of Crypto 2009*, pages 619–636, 2009.

A Proofs for Our Weak IND-CCA1-Secure IBE (Section 4.1)

To prove Theorem 4.3, which says that our IBE construction is weakly IND-CCA1 secure, we proceed through the following series of game transitions:

- Game_0. The honest weak IND-CCA1 game.
- Game_1. Switch to adding in a "duplicate" component in $G_3 \oplus G_4$ to the challenge ciphertext c_2^*; i.e., the value $g_3^{s'} g_4^{s' id}$. This is indistinguishable from Game_0 by subgroup decision.
- Game_2. Switch the $G_3 \oplus G_4$ component in c_2^* to be uniformly random. This is identical to Game_1 by parameter hiding.
- Game_3. Switch the keys returned by KeyExt to have random components in $H_3 \oplus H_4$ on $sk_{id,1}$ and on $sk_{id,2}$; i.e., values $h_3^{s'} h_4^{s''}$ (different values of s', s'' for $sk_{id,1}$ and $sk_{id,2}$). This is indistinguishable from Game_2 using a hybrid argument relying on subgroup decision and parameter hiding.

- Game_4. Switch from performing the decryption check with a term of the form $h_1^{t' id} h_2^{t'} h_5^{\gamma'} h_6^{\beta'}$ to using a term of the form $h_1^{t' id} h_2^{t'} h_3^{t'' id} h_4^{t''} h_5^{\gamma'} h_6^{\beta'}$. This is indistinguishable from Game_3 by subgroup decision.
- Game_5. Switch the Dec oracle to return $\perp$ on every query in which $c_2 \neq 1$, and 1 if $c_2 = 1$. This is indistinguishable from Game_4 by subgroup decision and parameter hiding.
- Game_6. Switch to encrypting a random message in the challenge ciphertext. This is indistinguishable from Game_5 by subgroup decision; furthermore, as there is now no information about the bit b, any adversary playing this game has advantage exactly zero.

Following this outline, we begin in Game_1 by adding a "duplicate" $G_3 \oplus G_4$ component to the ciphertext.

Game_0, $\boxed{\mathsf{Game}_1}$

1 $(N, G, H, G_T, e, \{g_i\}_{i=1}^6, \{h_i\}_{i=1}^6, \mu) \xleftarrow{\$} \mathsf{BilinearGen}(1^k, 6)$; $\mathbb{G} \leftarrow (N, G, H, G_T, e, \mu)$

2 $\alpha \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$, $A \leftarrow e(g_1, h_1)^\alpha$, $msk \leftarrow h_1^\alpha$

3 $(\mathsf{state}, M_0, M_1, id^*) \xleftarrow{\$} \mathcal{A}^{\mathsf{KeyExt},\mathsf{Dec}}(\mathbb{G})$

4 $b \xleftarrow{\$} \{0,1\}$

5 $s \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$, $\boxed{s, s' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}}$; $c_1^* \leftarrow M_b \cdot A^s$, $c_2^* \leftarrow g_1^s g_2^{s id^*}$, $\boxed{c_2^* \leftarrow g_1^s g_2^{s id^*} g_3^{s'} g_4^{s' id^*}}$

6 $b' \xleftarrow{\$} \mathcal{A}^{\mathsf{KeyExt}}(\mathsf{state}, (c_1^*, c_2^*))$

<u>Procedure $\mathsf{KeyExt}(id)$</u>

7 $t, t', \gamma, \gamma', \beta, \beta' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$

8 return $(sk_{id,1} \leftarrow h_1^\alpha \cdot h_1^{t id} \cdot h_2^t \cdot h_5^\gamma \cdot h_6^\beta, sk_{id,2} \leftarrow h_1^{t' id} \cdot h_2^{t'} \cdot h_5^{\gamma'} \cdot h_6^{\beta'})$

<u>Procedure $\mathsf{Dec}(id, (c_1, c_2))$</u>

9 $t', \gamma', \beta' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$

10 if $e(c_2, h_1^{t' id} h_2^{t'} h_5^{\gamma'} h_6^{\beta'}) \neq 1$ return $\perp$

11 return $c_1 \cdot e(c_2, msk)^{-1}$

Lemma A.1. *If the generalized correlated subgroup decision assumption and canceling hold in $\mathbb{G}$, then* Game_1 *is computationally indistinguishable from* Game_0.

Proof. We assume there exists an adversary $\mathcal{A}$ that can distinguish between Game_0 and Game_1 with some non-negligible advantage and use it to construct an adversary $\mathcal{B}$ that solves an instance of the generalized correlated subgroup decision problem with related non-negligible advantage. We invoke the instance of the assumption parameterized by sets $S_G := \{1, 2\}$, $S_H := \{1, 2, 5, 6; ((1, 2), (3, 4))\}$, $T_1 = \{(1, 2)\}$, and $T_2 = \{(1, 2), (3, 4)\}$, with challenge terms in G.

To start, $\mathcal{B}$ therefore receives as input the bilinear group $\mathbb{G} = (N, G, H, G_T, e, \mu)$, and elements

$$(g_1, g_2, h_1, h_2, h_5, h_6, h_{1,3} := h_1^t h_3^z, h_{2,4} := h_2^t h_4^z, T, \tilde{T}),$$

where either $(T, \tilde{T}) = (g_1^s, g_2^s)$ or $(T, \tilde{T}) = (g_1^s g_3^w, g_2^s g_4^w)$ for $t, z, s, w \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$. $\mathcal{B}$ then chooses a random $\alpha \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and implicitly sets $A := e(g_1, h_1)^\alpha$; it then gives $\mathbb{G}$ to $\mathcal{A}$. On KeyExt queries, $\mathcal{B}$ can use its knowledge of α to compute h_1^α and thus answer queries honestly. To answer decryption queries, $\mathcal{B}$ performs the check in line 10 and executes line 11 honestly.

Finally, to produce the challenge ciphertext, $\mathcal{B}$ picks $b \xleftarrow{\$} \{0,1\}$ and computes

$$c_1^* := M_b \cdot e(T, h_1)^\alpha \quad \text{and} \quad c_2^* := T \cdot \widetilde{T}^{id^*}.$$

If $(T, \widetilde{T}) = (g_1^s, g_2^s)$, then $c_1^* = M_b \cdot e(g_1, h_1)^{\alpha s}$ and $c_2^* = g_1^s \cdot g_2^{sid^*}$, and thus this is distributed identically to the honest c^* in Game_0. If instead $(T, \widetilde{T}) = (g_1^s g_3^w, g_2^s g_4^w)$, then

$$c_1^* = M_b \cdot e(g_1^s g_3^w, h_1)^\alpha = M_b \cdot e(g_1, h_1)^{\alpha s},$$

where this last equality follows from canceling, and $c_2^* = g_1^s \cdot g_2^{sid^*} \cdot g_3^w \cdot g_4^{wid^*}$, and thus (c_1^*, c_2^*) is distributed identically to the c^* in Game_1. At the end of the game, if $\mathcal{A}$ guesses it is in Game_0 then $\mathcal{B}$ therefore guesses that $(T, \widetilde{T}) = (g_1^s, g_2^s)$, and if $\mathcal{A}$ guesses it is in Game_1 then $\mathcal{B}$ guesses that $(T, \widetilde{T}) = (g_1^s g_3^w, g_2^s g_4^w)$. As $\mathcal{B}$ perfectly simulates the interaction that $\mathcal{A}$ expects in either game and furthermore guesses correctly whenever $\mathcal{A}$ does, $\mathcal{B}$ succeeds with an advantage negligibly different from that of $\mathcal{A}$, and thus succeeds with non-negligible advantage. □

Next, in Game_2, we switch to using a random component in $G_3 \oplus G_4$ as opposed to a duplicate component. This means switching one line of Game_1 as follows:

Game_1, $\boxed{\mathsf{Game}_2}$

$s, s' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$, $\boxed{s, s_3, s_4 \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}}$; $c_1^* \leftarrow M_b \cdot A^s$, $c_2^* \leftarrow g_1^s g_2^{sid^*} g_3^{s'} g_4^{s'id^*}$, $\boxed{c_2^* \leftarrow g_1^s g_2^{sid^*} g_3^{s_3} g_4^{s_4}}$

Lemma A.2. *If parameter hiding holds in $\mathbb{G}$, then Game_2 is information-theoretically indistinguishable from Game_1.*

Proof. Given the distribution $\mathcal{D}$ defined in Example 2.7 for $x = id^*$, one can simulate an honest interaction in Game_1, as it provides the id^*-correlated samples $S_1 := g_1^s g_2^{sid^*}$ and $S_2 := g_3^w g_4^{wid^*}$, which can be used to form $c_2^* := S_1 \cdot S_2$. By parameter hiding, S_2 is distributed identically to $g_3^w g_4^u$ for $u \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$, and thus Game_1 and Game_2 are identical. □

Next, in Game_3, we transition to adding in random components in $H_3 \oplus H_4$ to the keys. This means changing two lines of Game_2 as follows:

Game_2, $\boxed{\mathsf{Game}_3}$

$t, t', \gamma, \gamma', \beta, \beta' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$, $\boxed{t, t', t_3, t_4, t_3', t_4', \gamma, \gamma', \beta, \beta' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}}$

return $(sk_{id,1} \leftarrow h_1^\alpha \cdot h_1^{tid} \cdot h_2^t \cdot h_5^\gamma \cdot h_6^\beta, sk_{id,2} \leftarrow h_1^{t'id} \cdot h_2^{t'} \cdot h_5^{\gamma'} \cdot h_6^{\beta'})$,

$\boxed{\text{return } (sk_{id,1} \leftarrow h_1^\alpha \cdot h_1^{tid} \cdot h_2^t \cdot h_3^{t''id} \cdot h_4^{t''} \cdot h_5^\gamma \cdot h_6^\beta, sk_{id,2} \leftarrow h_1^{t'id} \cdot h_2^{t'} \cdot h_3^{t'''id} \cdot h_4^{t'''} \cdot h_5^{\gamma'} \cdot h_6^{\beta'})}$

To now show that adding in random $H_3 \oplus H_4$ components to extracted keys goes unnoticed, we proceed through a series of q hybrids, where q is the number of queries made to the KeyExt oracle. In the i-th hybrid, we answer the first i queries with additional component $h_3^{t'} h_4^{t''}$, and we answer the last $q-i$ queries without such components; in fact, in the reduction we answer the queries using id-correlated components in $H_3 \oplus H_4$, but we argue using parameter hiding that this is distributed identically to the keys in Game_3. We can therefore see that the first hybrid $\mathsf{Game}_{3,0}$ is equivalent to Game_2, while the last hybrid $\mathsf{Game}_{3,q}$ is equivalent to Game_3; to show the indistinguishability of Game_2 and Game_3, it therefore suffices to show the following lemma:

Lemma A.3. *If the generalized correlated subgroup decision assumption and parameter hiding hold in $\mathbb{G}$, then $\mathsf{Game}_{3,i}$ is computationally indistinguishable from $\mathsf{Game}_{3,i-1}$ for all i, $1 \leq i \leq q$.*

Proof. We break the transition from $\mathsf{Game}_{3,i-1}$ to $\mathsf{Game}_{3,i}$ into two nearly identical steps. In the first step, we change the i-th key to have a random component in $H_3 \oplus H_4$ on $sk_{id,1}$. In the second step, we also make this change on $sk_{id,2}$. We assume there exists an adversary $\mathcal{A}$ that, for some i, can distinguish between the first step and $\mathsf{Game}_{3,i-1}$ with some non-negligible advantage and use it to construct an adversary $\mathcal{B}$ that solves an instance of the generalized correlated subgroup decision problem with related non-negligible advantage (assuming parameter hiding holds). We invoke the instance of the assumption parameterized by sets $S_G := \{1, 2; ((1, 2), (3, 4))\}$, $S_H := \{1, 2, 5, 6; ((3, 4), (5, 6)), ((1, 2), (3, 4))\}$, $T_1 = \{(1, 2), (5, 6)\}$, and $T_2 = \{(1, 2), (3, 4), (5, 6)\}$, with challenge terms in H.

To start, $\mathcal{B}$ therefore receives as input the bilinear group $\mathbb{G} = (N, G, H, G_T, e, \mu)$ and elements

$$(g_1, g_2, h_1, h_2, h_5, h_6, g_{1,3} := g_1^s g_3^w, g_{2,4} := g_2^s g_4^w, h_{3,5} := h_3^a h_5^b, h_{4,6} := h_4^a h_6^b, h_{1,3} := h_1^r h_3^v, h_{2,4} := h_2^r h_4^v, T, \widetilde{T}),$$

where either $(T, \tilde{T}) = (h_1^t h_5^\gamma, h_2^t h_6^\gamma)$ or $(T, \tilde{T}) = (h_1^t h_3^z h_5^\gamma, h_2^t h_4^z h_6^\gamma)$ for $s, w, a, b, r, v, t, z, \gamma \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$. It then chooses a random $\alpha \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and implicitly sets $A := e(g_1, h_1)^\alpha$; it also gives $\mathbb{G}$ to $\mathcal{A}$. For the first $i - 1$ KeyExt queries, $\mathcal{B}$ picks $t, t', \delta, \phi, \sigma, \phi, \delta', \phi', \sigma', \phi' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and returns

$$sk_{id,1} := h_1^\alpha \cdot h_1^{tid} \cdot h_2^t \cdot h_{3,5}^\delta \cdot h_{4,6}^\psi \cdot h_5^\sigma h_6^\phi \quad \text{and}$$
$$sk_{id,2} := h_1^{t'id} \cdot h_2^{t'} \cdot h_{3,5}^{\delta'} \cdot h_{4,6}^{\psi'} \cdot h_5^{\sigma'} \cdot h_6^{\phi'}.$$

To respond to the i-th query, $\mathcal{B}$ instead chooses $\sigma, \phi, t', \sigma', \phi' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and returns

$$sk_{id,1} := h_1^\alpha \cdot T^{id} \cdot \widetilde{T} \cdot h_5^\sigma \cdot h_6^\phi \quad \text{and}$$
$$sk_{id,2} := h_1^{t'id} \cdot h_2^{t'} \cdot h_5^{\sigma'} \cdot h_6^{\phi'}.$$

For the rest of the queries, $\mathcal{B}$ picks $t, t', \sigma, \phi, \sigma', \phi' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and returns

$$sk_{id,1} := h_1^\alpha \cdot h_1^{tid} \cdot h_2^t \cdot h_5^\sigma \cdot h_6^\phi \quad \text{and}$$
$$sk_{id,2} := h_1^{t'id} \cdot h_2^{t'} \cdot h_5^{\sigma'} \cdot h_6^{\phi'}.$$

To respond to decryption queries, $\mathcal{B}$ picks $t, \sigma, \phi \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and checks that $e(c_2, h_1^{tid} h_2^t h_5^\sigma h_6^\phi) = 1$. If this check fails, it outputs $\perp$. Otherwise, it decrypts honestly using h_1^α and outputs the result.

Finally, to create the challenge ciphertext for message M_b and identity id^*, $\mathcal{B}$ computes

$$c_1^* := M_b \cdot e(g_{1,3}, h_1)^\alpha \quad \text{and} \quad c_2^* = g_{1,3}(g_{2,4})^{id^*}.$$

If $\mathcal{A}$ guesses it is in $\mathsf{Game}_{3,i-1}$, then $\mathcal{B}$ guesses that $(T, \tilde{T})$ has no H_3 or H_4 component, while if it guesses that it is in the game with the first step applied $\mathcal{B}$ guesses that it does have this additional component. To see that $\mathcal{B}$ guesses correctly whenever $\mathcal{A}$ does, we observe that if $(T, \tilde{T}) = (h_1^t h_5^\gamma, h_2^t h_6^\gamma)$ then, for the i-th query,

$$sk_{id,1} = h_1^\alpha \cdot h_1^{tid} \cdot h_2^t \cdot h_5^{\gamma id} \cdot h_5^\sigma \cdot h_6^\gamma \cdot h_6^\phi = h_1^\alpha \cdot h_1^{tid} \cdot h_2^t \cdot h_5^{\gamma id + \sigma} \cdot h_6^{\gamma + \phi} = h_1^\alpha \cdot h_1^{tid} \cdot h_2^t \cdot h_5^{\sigma'} \cdot h_6^{\phi'},$$

where σ' and ϕ' are distributed uniformly at random; this is therefore distributed identically to a key in Game_2. Similarly, if $(T, \tilde{T}) = (h_1^t h_3^z h_5^\gamma, h_2^t h_4^z h_6^\gamma)$ then, for the i-th query,

$$sk_{id,1} = h_1^\alpha \cdot T^{id} \cdot \tilde{T} \cdot h_5^\sigma \cdot h_6^\phi = h_1^\alpha \cdot h_1^{tid} \cdot h_2^t \cdot h_3^{zid} \cdot h_4^z \cdot h_5^{\gamma id} \cdot h_5^\sigma \cdot h_6^\gamma \cdot h_6^\phi = h_1^\alpha \cdot h_1^{tid} \cdot h_2^t \cdot h_3^{zid} \cdot h_4^z \cdot h_5^{\sigma'} \cdot h_6^{\phi'},$$

which is distributed identically to a key in Game_3, except an id-correlated sample is used in $H_3 \oplus H_4$ in place of a random sample. As knowledge of the distribution $\mathcal{D}$ in Example 2.7 allows one to simulate $\mathcal{A}$'s view, however, the requirement that $id \neq id^*$ means parameter hiding implies that this is in fact distributed identically to a key in Game_3. As $\mathcal{B}$ therefore perfectly simulates $\mathsf{Game}_{3,i-1}$ in the case that $(T, \tilde{T}) = (h_1^t h_5^\gamma, h_2^t h_6^\gamma)$ and perfectly simulates $sk_{id,1}$ keys in $\mathsf{Game}_{3,i}$ in the case that $(T, \tilde{T}) = (h_1^t h_3^z h_5^\gamma, h_2^t h_4^z h_6^\gamma)$, it succeeds in guessing whenever $\mathcal{A}$ does, and thus succeeds with non-negligible advantage.

The second step of this transition adds a random component onto $sk_{id,2}$ in an analogous way, and thus the reduction here is analogous to the one just presented (using the same instance of the generalized correlated subgroup decision assumption). □

Next, in Game_4, we change the decryption check as follows:

$$\mathsf{Game}_3, \boxed{\mathsf{Game}_4}$$

$$t', \gamma', \beta' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}, \boxed{t', t'', \gamma', \beta' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}}$$

$$\text{if } e(c_2, h_1^{t'id} h_2^{t'} h_5^{\gamma'} h_6^{\beta'}) \neq 1 \text{ return } \bot,$$

$$\boxed{\text{if } e(c_2, h_1^{t'id} h_2^{t'} h_3^{t''id} h_4^{t''} h_5^{\gamma'} h_6^{\beta'}) \neq 1 \text{ return } \bot}$$

Lemma A.4. *If the generalized correlated subgroup decision assumption holds in $\mathbb{G}$, then Game_4 is computationally indistinguishable from Game_3.*

Proof. We assume we have an adversary $\mathcal{A}$ that distinguishes between Game_3 and Game_4 with some non-negligible advantage, and use it to create an adversary $\mathcal{B}$ that solves an instance of the generalized correlated subgroup decision problem with related non-negligible advantage. We invoke the instance of the assumption parameterized by sets $S_G := \{1, 2; ((1,2),(3,4))\}$, $S_H := \{1, 2, 5, 6; ((3,4),(5,6)), ((1,2),(3,4))\}$, $T_1 = \{(1,2),(5,6)\}$, and $T_2 = \{(1,2),(3,4),(5,6)\}$, with challenge terms in H.

To start, $\mathcal{B}$ therefore receives as input the bilinear group $\mathbb{G} = (N, G, H, G_T, e, \mu)$ and elements

$$(g_1, g_2, h_1, h_2, h_5, h_6, g_{1,3} := g_1^s g_3^w, g_{2,4} := g_2^s g_4^w, h_{3,5} := h_3^a h_5^b, h_{4,6} := h_4^a h_6^b, h_{1,3} := h_1^r h_3^v, h_{2,4} := h_2^r h_4^v, T, \widetilde{T}),$$

where either $(T, \tilde{T}) = (h_1^t h_5^\gamma, h_2^t h_6^\gamma)$ or $(T, \tilde{T}) = (h_1^t h_3^z h_5^\gamma, h_2^t h_4^z h_6^\gamma)$ for $s, w, a, b, r, v, t, z, \gamma \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$. It then chooses a random $\alpha \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and implicitly sets $A := e(g_1, h_1)^\alpha$; it also gives $\mathbb{G}$ to $\mathcal{A}$.

To respond to KeyExt queries, $\mathcal{B}$ picks $t, t', \delta, \phi, \sigma, \phi, \delta', \phi', \sigma', \phi' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and returns

$$sk_{id,1} := h_1^\alpha \cdot h_1^{tid} \cdot h_2^t \cdot h_{3,5}^\delta \cdot h_{4,6}^\psi \cdot h_5^\sigma h_6^\phi \quad \text{and}$$
$$sk_{id,2} := h_1^{t'id} \cdot h_2^{t'} \cdot h_{3,5}^{\delta'} \cdot h_{4,6}^{\psi'} \cdot h_5^{\sigma'} \cdot h_6^{\phi'}.$$

To respond to decryption queries, $\mathcal{B}$ chooses $\sigma, \phi, t', t, \sigma', \phi' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and checks that

$$e(c_2, h_1^{tid} \cdot h_2^t \cdot T^{t'id} \cdot \widetilde{T}^{t'} \cdot h_5^\sigma \cdot h_6^\phi) = 1.$$

If this check fails, it outputs $\bot$. Otherwise, it decrypts honestly using h_1^α and outputs the result. If T and $\widetilde{T}$ have no $H_3 \oplus H_4$ components, this check matches the one in Game_3, and otherwise this matches the check in Game_4.

Finally, to create the challenge ciphertext for message M_b and identity id^*, $\mathcal{B}$ computes

$$c_1^* := M_b e(g_{1,3}, h_1)^\alpha \quad \text{and} \quad c_2^* = g_{1,3}(g_{2,4})^{id^*}.$$

If $\mathcal{A}$ guesses that it is in Game_3, $\mathcal{B}$ guesses that $(T, \widetilde{T}) = (h_1^t h_5^\gamma, h_2^t h_6^\gamma)$, and if $\mathcal{A}$ guesses that it is in Game_4, $\mathcal{B}$ guesses that $(T, \widetilde{T}) = (h_1^t h_3^z h_5^\gamma, h_2^t h_4^z h_6^\gamma)$. By our argument above, and the fact that $\mathcal{B}$ perfectly simulates either Game_3 or Game_4, $\mathcal{B}$ guesses correctly whenever $\mathcal{A}$ does and thus guesses with the same non-negligible advantage. □

Next, in Game_5, we switch to returning $\perp$ on all decryption queries, unless $c_2 = 1$ (in which case we return 1). As we will see, this reduction is where we crucially leverage the weak IND-CCA property that the parameters are not given to the attacker.

	Game_4	Game_5
9	if $e(c_2, h_1^{t' id} h_2^{t'} h_5^{\gamma'} h_6^{\beta'}) \neq 1$ return $\perp$	if $c_2 = 1$ return 1
10	return $c_1 \cdot e(c_2, msk)^{-1}$	return $\perp$

Lemma A.5. *If the generalized correlated subgroup decision assumption and parameter hiding hold in* $\mathbb{G}$*, then* Game_4 *is computationally indistinguishable from* Game_5*.*

Proof. Looking at the difference between the games, we can see that the only way for an adversary to distinguish between them is to produce a decryption query $(id, (c_1, c_2))$ for which $c_2 \neq 1$ but the decryption check $e(c_2, h_1^{tid} h_2^t h_3^{t'id} h_4^{t'} h_5^{\varrho} h_6^{\phi}) = 1$ passes. By parameter hiding, we argue that, given the elements that an adversary sees in the course of the game, this probability must be negligible unless c_2 is an element of $G_1 \oplus G_2$. If this is the case, we will use c_2 to break an instance of the correlated subgroup decision assumption.

We consider the instance of the generalized correlated subgroup decision assumption parameterized by sets $S_G := \{3, 4; ((1, 2), (3, 4))\}$, $S_H := \{3, 4, 5, 6; ((1, 2), (5, 6))$, $T_1 := \{(3, 4), (5, 6)\}$, and $T_2 := \{(1, 2), (3, 4), (5, 6)\}$, with challenge terms in H.

To start, $\mathcal{B}$ therefore receives as input the bilinear group $\mathbb{G} = (N, G, H, G_T, e, \mu)$, and elements

$$(g_3, g_4, h_3, h_4, h_5, h_6, g_{1,3} := g_1^s g_3^w, g_{2,4} := g_2^s g_4^w, h_{1,5} := h_1^a h_5^b, h_{2,6} := h_2^a h_6^b, T, \tilde{T}),$$

where either $(T, \tilde{T}) = (h_3^z h_5^{\gamma}, h_4^z h_6^{\gamma})$ or $(T, \tilde{T}) = (h_1^t h_3^z h_5^{\gamma}, h_2^t h_4^z h_6^{\gamma})$ for $s, w, a, b, z, \gamma, t \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$.

$\mathcal{B}$ implicitly sets $\alpha = a$ and gives $\mathbb{G}$ to $\mathcal{A}$. On KeyExt queries, $\mathcal{B}$ chooses random values $\sigma, \delta, \eta, \psi, \nu, \sigma', \delta', \eta', \psi', \nu' \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ and returns

$$sk_{id,1} := h_{1,5} \cdot h_{1,5}^{\eta id} \cdot h_{2,6}^{\eta} h_3^{\sigma} h_4^{\delta} h_5^{\psi} h_6^{\nu} \quad \text{and}$$
$$sk_{id,2} := h_{1,5}^{\eta' id} \cdot h_{2,6}^{\eta'} h_3^{\sigma'} h_4^{\delta'} h_5^{\psi'} h_6^{\nu'}.$$

By inspection, we can see that this produces keys that are distributed identically to the honest keys in both Game_4 and Game_5. For the challenge ciphertext, $\mathcal{B}$ similarly computes it honestly.

When $\mathcal{A}$ queries its Dec oracle on $(id, (c_1, c_2))$, $\mathcal{B}$ first checks that $e(c_2, h_5) = e(c_2, h_6) = 1$ and $e(c_2, h_3) = e(c_2, h_4) = 1$. If these checks pass, then c_2 is contained entirely in $G_1 \oplus G_2$. In this case, either $c_2 = 1$, in which case Game_4 and Game_5 return the same answer and thus are identical, or c_2 can be paired against T and $\tilde{T}$ to determine the presence of H_1 and H_2 terms; i.e., if $e(c_2, T) = 1$ then $T = h_3^z h_5^{\gamma}$, and if $e(c_2, T) \neq 1$ then $T = h_1^t h_3^z h_5^{\gamma}$. In the case that the checks pass and $c_2 \neq 1$, $\mathcal{B}$ can therefore break this variant of subgroup decision.

To argue that if $c_2 \neq 1$ this case must happen with non-negligible probability, we claim that $\mathcal{A}$ can, with only negligible probability, produce a query such that $e(c_2, h_1^{tid} h_2^t h_3^{t'id} h_4^{t'} h_5^{\varrho} h_6^{\phi}) = 1$ and $e(c_2, h_3) = e(c_2, h_4) = e(c_2, h_5) = e(c_2, h_6) = 1$ does *not* hold; this implies that the case we want will happen with overwhelming probability, and thus we are done. To see this, we again use the parameter hiding in Example 2.7: in $\mathcal{A}$'s view, only random elements of $H_3 \oplus H_4$ appear, and h_3 and h_4 are never used individually. One can thus simulate $\mathcal{A}$'s view using the distribution $\mathcal{D}$ in Example 2.7, and $h_3^{t' id} h_4^{t'}$ for a fixed id is distributed identically to a uniformly random element of $H_3 \oplus H_4$ by parameter hiding. Hence, $\mathcal{A}$ has only a negligible chance of passing the decryption check unless $c_2 \in G_1 \oplus G_2$, in which case either $c_2 = 1$, in which case the games are identical, or $c_2 \neq 1$, in which case $\mathcal{B}$ succeeds in breaking subgroup decision. $\square$

Finally, in Game_6, we switch to encrypting a random message in G_T.

$$\mathsf{Game}_5,\ \boxed{\mathsf{Game}_6}$$

$$s, s_3, s_4 \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z},\ \boxed{M \xleftarrow{\$} G_T};\ c_1^* \leftarrow M_b \cdot A^s,\ \boxed{c_1^* \leftarrow M \cdot A^s},\ c_2^* \leftarrow g_1^s g_2^{s id^*} g_3^{s_3} g_4^{s_4}$$

Lemma A.6. *If the generalized correlated subgroup decision assumption holds, then* Game_6 *is computationally indistinguishable from* Game_5*.*

Proof. We assume there exists an adversary $\mathcal{A}$ that distinguishes between these games with non-negligible advantage, and use $\mathcal{A}$ to construct an adversary $\mathcal{B}$ that solves an instance of the correlated subgroup decision assumption with related non-negligible advantage. We invoke the instance of this assumption parameterized by sets $S_G := \{3, 4; ((1, 2), (3, 4))\}$, $S_H := \{3, 4, 5, 6; ((1, 2), (5, 6))\}$, $T_1 = \{(3, 4), (5, 6)\}$, and $T_2 = \{(1, 2), (3, 4), (5, 6)\}$, with challenge terms in H.

$\mathcal{B}$ is therefore given as input the bilinear group $\mathbb{G} = (N, G, H, G_T, e, \mu)$, and elements

$$(g_3, g_4, h_3, h_4, h_5, h_6, g_{1,3} := g_1^s g_3^w, g_{2,4} := g_2^s g_4^w, h_{1,5} := h_1^{t'} h_5^z, h_{2,6} := h_2^{t'} h_6^z, T),$$

where either $T = h_3^r h_5^\gamma$ or $T = h_1^{\alpha'} h_3^r h_5^\gamma$ for $s, w, t', z, \alpha', r, \gamma \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$.

$\mathcal{B}$ implicitly sets $\alpha = t' + \alpha'$ (where α' is 0 if T has no h_1 component) and gives $\mathbb{G}$ to $\mathcal{A}$. On KeyExt queries, $\mathcal{B}$ chooses random values $\sigma, \sigma', \delta, \delta', \eta, \eta', \psi, \psi', \nu, \nu' \xleftarrow{\$} \mathbb{Z}_N$ and returns

$$sk_{id,1} := T \cdot h_{1,5} \cdot h_{1,5}^{\eta id} \cdot h_{2,6}^{\eta} h_3^{\sigma} h_4^{\delta} h_5^{\psi} h_6^{\nu},$$

$$sk_{id,2} := h_{1,5}^{\eta' id} \cdot h_{2,6}^{\eta'} h_3^{\sigma'} h_4^{\delta'} h_5^{\psi'} h_6^{\nu'}.$$

By inspection, we can see that this produces properly distributed keys for both Game_5 and Game_6. On decryption queries, $\mathcal{B}$ simply replies with $\perp$ whenever $c_2 \neq 1$ and with 1 whenever $c_2 = 1$. This also matches the specifications of both Game_5 and Game_6.

Finally, to form the challenge ciphertext, $\mathcal{B}$ chooses random values $\beta, \phi \xleftarrow{\$} \mathbb{Z}_N$ and computes

$$c_1^* := M_b e(g_{1,3}, h_{1,5}) \quad \text{and} \quad c_2^* := g_{1,3} \cdot g_{2,4}^{id^*} g_3^{\beta} g_4^{\phi}.$$

Now, if $T = h_3^r h_5^\gamma$, then $\alpha = t'$, and this is a properly distributed encryption of M_b as in Game_5. If $T = h_1^{\alpha'} h_3^r h_5^\gamma$, however, then $\alpha = t' + \alpha'$ for a fresh random value t', which means, using the fact that the message space is the subgroup generated by $e(g_1, h_1)$, this is distributed as an encryption of a random message as in Game_6. If $\mathcal{B}$ therefore guesses that $T = h_3^r h_5^\gamma$ when $\mathcal{A}$ guesses it is in Game_5, and that $T = h_1^{\alpha'} h_3^r h_5^\gamma$ when $\mathcal{A}$ guesses it is in Game_6 then, because $\mathcal{B}$ has furthermore perfectly simulated honest interactions in either game, $\mathcal{B}$ succeeds in guessing with the same non-negligible advantage as $\mathcal{A}$. □

As there is no longer any information about M_b, and thus the bit b, in the challenge ciphertext (or anywhere), $\mathcal{A}$ therefore has advantage exactly zero in Game_6. Furthermore, as each game was (at least) computationally indistinguishable from the previous one, $\mathcal{A}$ can have at most negligibly different advantage in each, and thus must have negligible advantage in the weak IND-CCA1 game.