Identity-based encryption with (almost) tight security in the multi-instance, multi-ciphertext setting

Dennis Hofheinz*, Jessica Koch†, and Christoph Striecks‡

Karlsruhe Institute of Technology, Germany,
{Dennis.Hofheinz,Jessica.Koch,Christoph.Striecks}@kit.edu

Abstract

We construct an identity-based encryption (IBE) scheme that is tightly secure in a very strong sense. Specifically, we consider a setting with many instances of the scheme and many encryptions per instance. In this setting, we reduce the security of our scheme to a variant of a simple assumption used for a similar purpose by Chen and Wee (Crypto 2013). The security loss of our reduction is $\mathbf{O}(k)$ (where k is the security parameter). Our scheme is the first IBE scheme to achieve this strong flavor of tightness under a simple assumption.

Technically, our scheme is a variation of the IBE scheme by Chen and Wee. However, in order to "lift" their results to the multi-instance, multi-ciphertext case, we need to develop new ideas. In particular, while we build on (and extend) their high-level proof strategy, we deviate significantly in the low-level proof steps.

1 Introduction

Tight security. For many cryptographic primitives, we currently cannot prove security directly. Hence, we typically *reduce* the security of a given scheme to the hardness of a computational problem, in the sense that every successful attack on the scheme yields a successful problem solver. Now it is both a theoretically and practically interesting question to look at the *loss* of such a reduction. Informally, the loss of a reduction quantifies the difference between the success of a hypothetical attacker on the cryptographic scheme, and the success of the derived problem solver. From a theoretical perspective, for instance, the loss of a reduction can also be viewed as a quantitative measure of (an upper bound for) the "distance" between primitive and assumption. But "tight" (or, "loss-free") reductions are also desirable from a practical perspective: the tighter a reduction, the better are the security guarantees we can give for a specific instance of the scheme. Hence, we can recommend smaller keylengths (which lead to more efficiency) for schemes with tighter security reduction.

However, in most practical usage scenarios, a cryptographic primitive is used multiple times. (For instance, in a typical multi-user encryption scenario, many instances of the encryption scheme are used to produce even more ciphertexts.) Hence, tight security reductions become particularly meaningful when they reduce an attacker on the whole system (with many instances of the cryptographic scheme) to a problem solver. In fact, while for many primitives (such as secret-key [2] or public-key [3] encryption), one-instance security is known to imply multi-instance security, the corresponding security guarantees for concrete schemes may indeed vanish in the number of instances [2].

Existing tightly secure schemes. The loss of security reductions has been considered explicitly by Bellare et al. [2] for the case of encryption schemes. The first "somewhat tight"

*Dennis Hofheinz was supported by DFG grants GZ HO 4534/2-2 and GZ HO 4534/4-1.
†Jessica Koch was supported by BMBF project "KASTEL".
‡Christoph Striecks was supported by DFG grant GZ HO 4534/2-2.

reductions (whose loss is independent of the number of instances of the scheme, but not of the number of ciphertexts) for public-key encryption (PKE) schemes could be given in [4]. In the following years, more tight (or somewhat tight) reductions for encryption schemes were constructed in the random oracle model [14, 10, 7], or from "q-type" assumptions [15, 16].[1]

However, only recently, the first PKE schemes emerged [18, 1, 20] whose tight security (in the multi-instance, multi-ciphertext setting) can be proved under simple assumptions in the standard model.[2] Even more recently, *identity-based* encryption (IBE) schemes with "somewhat tight" security (under simple assumptions) have been constructed [11, 6]. (This required new techniques, since it is not clear how to extend the techniques of [18, 1, 20] to the IBE setting.) In this case, "somewhat tight" means that their security reduction loses only a small multiplicative factor, but still considers the standard IBE security experiment [9] with one encryption and one instance of the scheme. Nonetheless, while the IBE schemes from [11, 6] are not proved tightly secure in a multi-user, multi-ciphertext setting, these schemes imply tightly secure PKE schemes (even in the multi-user, multi-ciphertext setting) when plugged into the transformations of [9, 18, 20].[3]

Our contribution. In this work, we construct the first IBE scheme with an almost tight security reduction in the multi-instance, multi-ciphertext scenario. Our reduction is only almost tight, since it loses a factor of $\mathbf{O}(k)$, where k is the security parameter. However, we stress that this loss is independent of the number of ciphertexts, revealed user secret keys, or instances of the scheme. In our security reduction, we rely on a computational assumption in composite-order pairing-friendly groups; this assumption is a variant of an assumption used by Chen and Wee [11] for their IBE scheme, and in particular simple in the above sense. We note that a conversion to the prime-order setting using the techniques from [17, 21, 13, 19] (see also [5]) seems plausible—specifically since Chen and Wee [11] already describe such a conversion for their assumption—, but we leave such a conversion as an open problem.

Our approach. Our scheme is a variant of the IBE scheme by Chen and Wee [11] (which is almost tightly secure in the one-instance, one-ciphertext setting), and our proof strategy draws heavily from theirs. Hence, to describe our techniques, let us first briefly sketch their strategy.

In a nutshell, Chen and Wee start with a real security game, in which an adversary A receives a master public key mpk of the scheme, as well as access to arbitrarily many user secret keys usk_{id} for adversarially chosen identities id. At some point, A selects a fresh challenge identity id^* and two messages M_0^*, M_1^*, and then receives the encryption $C_{id^*}^* \leftarrow \mathsf{Enc}(mpk, id^*, M_b)$ (under identity id^*) of one of these messages. After potentially querying more user secret keys (for identities $id \neq id^*$), A eventually outputs a guess b^* for b. If $b^* = b$, we say that A wins. Chen and Wee then show security by gradually changing this game (being careful not to significantly decrease A's success), until A trivially cannot win (except by guessing).

As a first preparatory change, Chen and Wee use the user secret key usk_{id^*} to construct the challenge ciphertext $C_{id^*}^*$. (This way, the encryption random coins for $C_{id^*}^*$ do not have to be known to the security game.) Additionally $C_{id^*}^*$ is now of a special, "pseudo-normal" form that will later enable a gradual randomization of the encrypted message. The core of the proof then consists of a number of hybrid steps, in which the distribution of all generated user secret keys (including the user secret key usk_{id^*} used to generate $C_{id^*}^*$) is modified. Concretely, in the

[1] A "q-type" assumption may depend on the size of the investigated cryptographic system. (That is, larger cryptographic systems may only be secure under a stronger instance of the assumption.) Hence, a tight reduction (even in a multi-instance scenario) to a q-type assumption may not yield security guarantees that are independent of the number of users.

[2] A "simple" assumption is defined through a security game in which an adversary first gets a challenge whose size only depends on the security parameter, and must then output a unique solution without further interaction. Examples of simple assumptions are DLOG, DDH, or RSA, but not Strong Diffie-Hellman [8] or q-ABDHE [15].

[3] More specifically, Boneh and Franklin [9] mention (and attribute this observation to Naor) that every IBE scheme can be viewed as a signature scheme. The signature schemes thus derived from [11, 6] are then suitable for the conversions of [18, 20], yielding PKE schemes tightly secure in the multi-user, multi-ciphertext setting.

i-th hybrid game, each used usk_{id} contains an additional "blinding term" of the form $R(id|_i)$, where $id|_i$ is the i-bit prefix of id, and R is a truly random function. Eventually, each user secret key usk_{id} will be fully randomized by a truly random value $R(id)$. In particular, at this point, the key usk_{id^*} used to prepare $C^*_{id^*}$ is blinded by a fresh random value $R(id^*)$. By the special "pseudo-normal" form of $C^*_{id^*}$, this means that the corresponding encrypted message is also blinded, and A's view is finally independent of the challenge bit b.

We keep this high-level proof structure, extending it of course to multiple ciphertexts and multiple instances of the scheme. However, as we will explain below, the way Chen and Wee gradually introduce the blinding terms $R(id|_i)$ does not immediately extend to many ciphertexts or instances; hence, we need to deviate from their proof strategy here.

The problem. Specifically, Chen and Wee move from the $(i-1)$-th to the i-th hybrid through a single reduction as follows: first, they guess the i-th bit id^*_i of the challenge identity id^*. Then, they set up things such that

(a) all user secret keys for identities id with $id_i = id^*_i$ (i.e., that coincide in the i-th bit with id^*) behave as in the previous hybrid (i.e., carry a blinding term $R(id|_{i-1})$),

(b) all user secret keys for identities id with $id_i = 1 - id^*_i$ carry a blinding term of $R(id|_{i-1}) \cdot R'(id|_{i-1})$. Depending on the input of the reduction, we have either that $R' = 1$ (such that the overall blinding term is $R(id|_{i-1})$), or that R' is an independently random function. (In particular, all usk_{id} with $id_i = 1 - id^*_i$ contain an embedded computational challenge R'.)

Depending on whether or not $R' = 1$, this setup simulates the $(i-1)$-th or the i-th hybrid. However, we remark that the setup of Chen and Wee only allows to generate "pseudo-normal" challenge ciphertexts $C^*_{id^*}$ for identities id^* with the initially guessed i-th bit id^*_i. (Intuitively, any pseudo-normal ciphertext for an identity id with $id_i = 1 - id^*_i$ would "react with" an additional blinding term $R'(id|_{i-1})$ in usk_{id}, allowing to trivially solve the computational challenge.)

Hence, in their i-th game hop, only challenge ciphertexts for identities with the same i-th bit can be generated. Thus, their approach cannot in any obvious way be extended to multiple challenge ciphertexts for different identities. (For similar reasons, a generalization to multiple instances of the scheme fails.)

Our solution. In order to move from the $(i-1)$-th to the i-th hybrid, we thus follow a different strategy that involves three reductions. The main technical ingredient in our case is the ability to distribute the blinding terms $R(id|_i)$ in user secret keys into two different "compartments" (i.e., subgroups) of the composite-order group we are working in. (In particular, a term $R(id|_i)$ in one compartment can be changed independently of terms in the other compartment.)

More specifically, recall that in the $(i-1)$-th hybrid, all user secret keys carry an additional $R(id|_{i-1})$ blinding term, and all challenge ciphertexts are pseudo-normal (in the sense that they "react with" the blinding terms in user secret keys). In our first step, we move all blinding terms $R(id|_{i-1})$ in the usk_{id} into the two compartments, depending on the i-th bit of id. (That is, if $id_i = 0$, then the corresponding blinding term $R(id|_{i-1})$ goes into the first compartment, and if $id_i = 1$, then it goes into the second.)

In our second step, we can now treat the embedded blinding terms for $id_i = 0$ and $id_i = 1$ separately. In particular, since these cases are now "decoupled" by being in different compartments, we can completely re-randomize the underlying random function R in exactly one of those compartments. (This does not lead to trivial distinctions of the computational challenge since we do not introduce *new* blinding terms that would "react with" pseudo-normal ciphertexts and thus become easily detectable. Instead, we simply *decouple* existing blinding terms in different subgroups.) Note however that since now different random functions, say, $\widehat{R}$ and $\widetilde{R}$, determine the blinding terms used for identities with $id_i = 0$ and $id_i = 1$, we essentially obtain blinding terms that depend on the first i (and not only $i-1$) bits of id.

Finally, we revert the first change and move all blinding terms in the usk_{id} into one compartment. In summary, this series of three moves has thus created blinding terms that depend on the first i bits of id. Thus, we have moved to the i-th hybrid. If we follow the high-level strategy

of Chen and Wee again, this yields a sequence of $\mathbf{O}(k)$ reductions that show the security of our IBE scheme. (From a conceptual perspective, it might also be interesting to note that none of our reductions needs to *guess*, e.g., an identity bit.)

Outline of the paper. After introducing some preliminary definitions in Section 2, we explain the necessary algebraic structure (mentioned in the "compartment discussion" above) of "extended nested dual system groups" (ENDSGs) in Section 3. (This structure extends a similar structure of Chen and Wee [11].) In Section 4, we present our IBE scheme from ENDSGs, and in Section 5, we show how to instantiate ENDSGs in composite-order pairing-friendly groups.

2 Preliminaries

Notation. For $n \in \mathbb{N}$, let $[n] := \{1, \ldots, n\}$, and let $k \in \mathbb{N}$ be the security parameter. For a finite set $\mathcal{S}$, we denote by $s \leftarrow \mathcal{S}$ the process of sampling s uniformly from $\mathcal{S}$. For an algorithm A, let $y \leftarrow A(k, x)$ be the process of running A on input k, x with access to uniformly random coins and assigning the result to y. (We may omit to mention the k-input explicitly and assume that all algorithms take k as input.) To make the random coins r explicit, we write $A(k, x; r)$. We say an algorithm A is probabilistic polynomial time (PPT) if the running time of A is polynomial in k. A function $f : \mathbb{N} \to \mathbb{R}$ is negligible if it vanishes faster than the inverse of any polynomial (i.e., if $\forall c \exists k_0 \forall k \geq k_0 : |f(k)| \leq 1/k^c$). Further, we write vectors in bold font, e.g., $\mathbf{v} = (v_1, \ldots, v_n)$ for a vectors of length $n \in \mathbb{N}$ and with components $v_1, \ldots, v_n$. (We may also write $\mathbf{v} = (v_i)_{i \in [n]}$ or even $\mathbf{v} = (v_i)_i$ in this case.) In the following, we use a *component-wise* multiplication of vectors, i.e., $\mathbf{v} \cdot \mathbf{v}' = (v_1, \ldots, v_n) \cdot (v'_1, \ldots, v'_n) = (v_1 \cdot v'_1, \ldots, v_n \cdot v'_n)$. Further, we write $\mathbf{v}^j := (v_1^j, \ldots, v_n^j)$, for $j \in \mathbb{N}$, and $\mathbf{v}_{-i} := (v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)$, for $i \in [n]$, and $s^{\mathbf{v}} := (s^{v_1}, \ldots, s^{v_n})$. For two random variables X, Y, we denote with $\mathsf{SD}(X ; Y)$ is the statistical distance of X and Y. We might also say that X and Y are ε-close if $\mathsf{SD}(X ; Y) \leq \varepsilon$.

Identity-based encryption. An identity-based encryption (IBE) scheme IBE with identity space $\mathcal{ID}$ and message space $\mathcal{M}$ consists of the five PPT algorithms $\mathsf{Par}, \mathsf{Gen}, \mathsf{Ext}, \mathsf{Enc}, \mathsf{Dec}$. Parameter sampling $\mathsf{Par}(k, n)$, on input a security parameter k and an identity length parameter $n \in \mathbb{N}$, outputs public parameters pp and secret parameters sp. (We assume that Ext, Enc, and Dec have implicitly access to pp.) Key generation $\mathsf{Gen}(pp, sp)$, on input pp and sp, outputs a master public key mpk and a master secret key msk. User secret key extraction $\mathsf{Ext}(msk, id)$, given msk and an identity $id \in \mathcal{ID}$, outputs a user secret key usk_{id} associated with id. Encryption $\mathsf{Enc}(mpk, id, M)$, given mpk, an identity $id \in \mathcal{ID}$, and a message $M \in \mathcal{M}$, outputs an id-associated ciphertext C_{id}. Decryption $\mathsf{Dec}(usk_{id}, C_{id})$, given usk_{id} for an identity id, and ciphertext C_{id}, outputs $M \in \mathcal{M} \cup \{\perp\}$. For correctness, we require that for any $k, n \in \mathbb{N}$, for all $(pp, sp) \leftarrow \mathsf{Par}(k, n)$, for all $(mpk, msk) \leftarrow \mathsf{Gen}(pp, sp)$, for all $id \in \mathcal{ID}$, for all $usk_{id} \leftarrow \mathsf{Ext}(msk, id)$, for all $M \in \mathcal{M}$, and for all $C_{id} \leftarrow \mathsf{Enc}(mpk, id, M)$, Dec satisfies $\mathsf{Dec}(usk_{id}, C_{id}) = M$. For security, we define multi-instance, multi-ciphertext IBE security, dubbed (μ, q)-IBE-IND-CPA security, for $(\mu, q) \in \mathbb{N}^2$, as follows.

(Weak) (μ, q)-IBE-IND-CPA security. An IBE scheme IBE defined as above is (μ, q)-IBE-IND-CPA-secure if and only if any PPT adversary A succeeds in the following experiment only with probability at most negligibly larger than $1/2$. Let $\mathsf{Enc}'(mpk, id, b, M_0, M_1)$ be a PPT auxiliary encryption oracle that, given a master public key mpk, a challenge identity $id \in \mathcal{ID}$, a bit $b \in \{0, 1\}$, and two messages $M_0, M_1 \in \mathcal{M}$, outputs a challenge ciphertext $C_{id} \leftarrow \mathsf{Enc}(mpk, id, M_b)$. First, A gets honestly generated public parameter pp and master public keys $(mpk_1, \ldots, mpk_\mu)$. During the experiment, A may adaptively query $\mathsf{Ext}(msk_j, \cdot)$-oracles and $\mathsf{Enc}'(mpk_j, \cdot, b, \cdot, \cdot)$-oracles, for corresponding mpk_j, msk_j and a (uniform) bit $b \leftarrow \{0, 1\}$, for all $j \in [\mu]$. Eventually, A outputs a guess b^*. We say that A is valid if and only if A never queries an $\mathsf{Ext}(msk_j, \cdot)$ oracle on an identity id for which it

Experiment $\mathsf{Exp}^{(\mu,q)\text{-ibe-ind-cpa}}_{\mathsf{IBE},A}(k,n)$
$(pp, sp) \leftarrow \mathsf{Par}(k,n)$
$(mpk_j, msk_j)_{j\in[\mu]} \leftarrow (\mathsf{Gen}(pp,sp))^{\mu}$
$b \leftarrow \{0,1\}$
$b^* \leftarrow A^{(\mathsf{Ext}(msk_j,\cdot),\mathsf{Enc}'(mpk_j,\cdot,b,\cdot,\cdot))_{j\in[\mu]}}(pp,(mpk_j)_{j\in[\mu]})$
if A is valid and $b = b^*$ then return 1 else return 0

Figure 1: The (μ, q)-IBE-IND-CPA security experiment.

has already queried the corresponding $\mathsf{Enc}'(mpk_j,\cdot,b,\cdot,\cdot)$ oracle (and vice versa); each message pair A selected as input to Enc' contained only equal-length messages; and A has only queried its Enc'-oracles at most q times per j-instance. We say that A succeeds if and only if A is valid and $b = b^*$. Concretely, the previous described experiment is given in Figure 1 and denoted $\mathsf{Exp}^{(\mu,q)\text{-ibe-ind-cpa}}_{\mathsf{IBE},A}$. Further, we define the advantage function for any PPT A as $\mathsf{Adv}^{(\mu,q)\text{-ibe-ind-cpa}}_{\mathsf{IBE},A}(k,n) := |\Pr\left[\mathsf{Exp}^{(\mu,q)\text{-ibe-ind-cpa}}_{\mathsf{IBE},A}(k,n) = 1\right] - 1/2\,|$.

Furthermore, we call IBE *weakly* (μ, q)-IBE-IND-CPA secure if and only if $\mathsf{Adv}^{(\mu,q)\text{-ibe-ind-cpa}}_{\mathsf{IBE},A}$ is negligible for all *weak* PPT adversaries A. Here, A is weak if it never requests challenge ciphertexts for the same scheme instance and identity twice (i.e., if it never queries any $\mathsf{Enc}'(mpk_j,\cdot,b,\cdot,\cdot)$ oracle twice with the same identity id).

Finally, we remark that the one-instance, one-ciphertext notion $(1, 1)$-IBE-IND-CPA is the standard notion of IBE security considered in, e.g., [9, 11, 6].

Pairings. Let G, H, G_T be cyclic groups of order N. A *pairing* $e : G \times H \to G_T$ is a map that is *bilinear* (i.e., for all $g, g' \in G$ and $h, h' \in H$, we have $e(g \cdot g', h) = e(g, h) \cdot e(g', h)$ and $e(g, h \cdot h') = e(g, h) \cdot e(g, h')$), *non-degenerate* (i.e., for generators $g \in G, h \in H$, we have that $e(g, h) \in G_T$ is a generator), and *efficiently computable*.

3 Extended nested dual system groups

(Nested) dual system groups. Nested dual system groups (NDSG) [11] can be seen as a variant of dual system groups (DSG) [12] which itself are based on the dual system framework introduced by Waters [21]. NDSGs were recently defined by Chen and Wee and enabled to prove the first IBE (almost) tightly and fully secure under simple assumptions. In the following, based on NDSGs, we construct a new notion we call extended nested dual system groups.

A variant of nested dual system groups. We introduce a variant of Chen and Wee's nested dual system groups (NDSG) [11], dubbed extended NDSG (ENDSG). (Mainly, we re-use and extend the notions from [11].) Further, let $\mathsf{G}(k, n')$ be a group generator that, given integers k and n', generates the tuple $(G, H, G_T, N, (g_{p_1}, \ldots, g_{p_{n'}}), (h_{p_1}, \ldots, h_{p_{n'}}), g, h, e)$, for a pairing $e : G \times H \to G_T$, for composite-order groups G, H, G_T, all of known group order $N = p_1 \cdots p_{n'}$, for k-bit primes $(p_i)_i$ and integer $n' \in \mathbf{O}(1)$. Further, g and h are generators of G and H, and $(g_{p_i})_i$ and $(h_{p_i})_i$ are generators of the (proper) subgroups $G_{p_i} \subset G$ and $H_{p_i} \subset H$ of order $|G_{p_i}| = |H_{p_i}| = p_i$, respectively. In this setting, an ENDSG ENDSG consists of algorithms $\mathsf{SampP}, \mathsf{SampG}, \mathsf{SampH}, \widehat{\mathsf{SampG}}, \widetilde{\mathsf{SampG}}$:

Parameter sampling. $\mathsf{SampP}(k, n)$, given security parameter k and parameter $n \in \mathbb{N}$, samples $(G, H, G_T, N, (g_{p_1}, \ldots, g_{p_{n'}}), (h_{p_1}, \ldots, h_{p_{n'}}), g, h, e) \leftarrow \mathsf{G}(k, n')$, for a constant integer n' determined by SampP, and outputs public parameters $pp = (G, H, G_T, N, g, h, e, m, n, pars)$ and secret parameters $sp = (\widehat{h}, \widetilde{h}, \widehat{pars}, \widetilde{pars})$, where $m : H \to G_T$ is a linear map, $\widehat{h}, \widetilde{h}$ are nontrivial H-elements, and $pars, \widehat{pars}, \widetilde{pars}$ may contain arbitrary additional information used by $\mathsf{SampG}, \mathsf{SampH}$, and $\widehat{\mathsf{SampG}}$ and $\widetilde{\mathsf{SampG}}$.

G-group sampling. $\mathsf{SampG}(pp)$, given parameter pp, outputs $\mathbf{g} = (g_0, \ldots, g_n) \in G^{n+1}$.

H-group sampling. $\mathsf{SampH}(pp)$, given parameter pp, outputs $\mathbf{h} = (h_0, \ldots, h_n) \in H^{n+1}$.

Semi-functional G-group sampling 1. $\widehat{\mathsf{SampG}}(pp, sp)$, given parameters pp and sp, outputs $\widehat{\mathbf{g}} = (\widehat{g}_0, \ldots, \widehat{g}_n) \in G^{n+1}$.

Semi-functional G-group sampling 2. $\widetilde{\mathsf{SampG}}(pp, sp)$, given parameters pp and sp, outputs $\widetilde{\mathbf{g}} = (\widetilde{g}_0, \ldots, \widetilde{g}_n) \in G^{n+1}$.

Correctness of ENDSG. For correctness, for all $k \in \mathbb{N}$, for all integers $n = n(k) > 1$, for all pp, where pp is the first output of $\mathsf{SampP}(k, n)$, we require:

Associativity. For all $(g_0, \ldots, g_n) \leftarrow \mathsf{SampG}(pp)$ and for all $(h_0, \ldots, h_n) \leftarrow \mathsf{SampH}(pp)$, we have $e(g_0, h_i) = e(g_i, h_0)$, for all $i \in [n]$.

Projective. For all $s \leftarrow \mathbb{Z}_N^*$, for all g_0 which is the first output of $\mathsf{SampG}(pp; s)$, for all $h \in H$, we have $m(h)^s = e(g_0, h)$.

Security of ENDSG. For security, for all $k \in \mathbb{N}$, for all integers $n = n(k) > 1$, for all $(pp, sp) \leftarrow \mathsf{SampP}(k, n)$, we require:

Orthogonality. For m specified in pp, for $\widehat{h}, \widetilde{h}$ specified in sp, we have $m(\widehat{h}) = m(\widetilde{h}) = 1$. For g_0, $\widehat{g}_0$, and $\widetilde{g}_0$ that are the first outputs of $\mathsf{SampG}(pp)$, $\widehat{\mathsf{SampG}}(pp, sp)$, and $\widetilde{\mathsf{SampG}}(pp, sp)$, respectively, we have that $e(g_0, \widehat{h}) = 1$, $e(g_0, \widetilde{h}) = 1$, $e(\widehat{g}_0, \widetilde{h}) = 1$, and $e(\widetilde{g}_0, \widehat{h}) = 1$.

G- and H-subgroups. The outputs of SampG, $\widehat{\mathsf{SampG}}$, and $\widetilde{\mathsf{SampG}}$ are distributed uniformly over the generators of different nontrivial subgroups of G^{n+1} (that only depend on pp) of coprime order, respectively, while the output of SampH is uniformly distributed over the generators of a nontrivial subgroup of H^{n+1} (that only depends on pp).

Non-degeneracy. For $\widehat{h}$ specified in sp and for $\widehat{g}_0$ which is the first output of $\widehat{\mathsf{SampG}}(pp, sp)$, it holds that $e(\widehat{g}_0, \widehat{h})$ is uniformly distributed over the generators of a nontrivial subgroup of G_T (that only depends on pp). Similarly, $e(\widetilde{g}_0, \widetilde{h})$ is uniformly distributed over the generators of a nontrivial subgroup of G_T (that only depends on pp), where $\widetilde{h}$ is specified in sp and $\widetilde{g}_0$ is the first output of $\widetilde{\mathsf{SampG}}(pp, sp)$.

Left-subgroup indistinguishability 1 (LS1). For any PPT adversary D, we have that the function

$$\mathsf{Adv}^{\mathrm{ls1}}_{\mathsf{ENDSG},\mathsf{G},D}(k, n) := |\Pr[D(pp, \mathbf{g}) = 1] - \Pr[D(pp, \mathbf{g}\widehat{\mathbf{g}}) = 1]|$$

is negligible in k, where $\mathbf{g} \leftarrow \mathsf{SampG}(pp)$, $\widehat{\mathbf{g}} \leftarrow \widehat{\mathsf{SampG}}(pp, sp)$.

Left-subgroup indistinguishability 2 (LS2). For any PPT adversary D, we have that the function

$$\mathsf{Adv}^{\mathrm{ls2}}_{\mathsf{ENDSG},\mathsf{G},D}(k, n) := |\Pr\left[D(pp, \widehat{h}\widetilde{h}, \mathbf{g}'\widehat{\mathbf{g}}', \mathbf{g}\widehat{\mathbf{g}}) = 1\right] - \Pr\left[D(pp, \widehat{h}\widetilde{h}, \mathbf{g}'\widehat{\mathbf{g}}', \mathbf{g}\widetilde{\mathbf{g}}) = 1\right]|$$

is negligible in k, where $\mathbf{g}, \mathbf{g}' \leftarrow \mathsf{SampG}(pp)$, $\widehat{\mathbf{g}}, \widehat{\mathbf{g}}' \leftarrow \widehat{\mathsf{SampG}}(pp, sp)$, $\widetilde{\mathbf{g}} \leftarrow \widetilde{\mathsf{SampG}}(pp, sp)$, for $\widehat{h}$ and $\widetilde{h}$ specified in sp.

Nested-hiding indistinguishability (NH). For any PPT adversary D, for all integers $q' = q'(k)$, the function

$$\mathsf{Adv}^{\mathrm{nh}}_{\mathsf{ENDSG},\mathsf{G},D}(k,n,q') := \max_{i\in[\lfloor \frac{n}{2} \rfloor]} \Big(\big| \Pr\left[D(pp, \widehat{h}, \widetilde{h}, \widehat{\mathbf{g}}_{-(2i-1)}, \widetilde{\mathbf{g}}_{-2i}, (\mathbf{h}_1, \ldots, \mathbf{h}_{q'})) = 1\right] - \Pr\left[D(pp, \widehat{h}, \widetilde{h}, \widehat{\mathbf{g}}_{-(2i-1)}, \widetilde{\mathbf{g}}_{-2i}, (\mathbf{h'}_1, \ldots, \mathbf{h'}_{q'})) = 1\right] \big| \Big),$$

is negligible in k, where $\widehat{\mathbf{g}} \leftarrow \widehat{\mathsf{SampG}}(pp, sp)$, $\widetilde{\mathbf{g}} \leftarrow \widetilde{\mathsf{SampG}}(pp, sp)$, and

$$\mathbf{h}_{i'} := (h_{i',0}, \ldots, h_{i',n}) \leftarrow \mathsf{SampH}(pp),$$

$$\mathbf{h'}_{i'} := (h_{i',0}, \ldots, h_{i',2i-1} \cdot (\widehat{h})^{\widehat{\gamma}_{i'}}, h_{i',2i} \cdot (\widetilde{h})^{\widetilde{\gamma}_{i'}}, \ldots, h_{i',n}),$$

for $\widehat{h}, \widetilde{h}$ specified in sp, for $\widehat{\gamma}_{i'}, \widetilde{\gamma}_{i'} \leftarrow \mathbb{Z}^*_{\mathsf{ord}(H)}$, and for all $i' \in [q']$.

(Informal) comparison of NDSGs and ENDSGs. Loosely speaking, in contrast to the NDSGs from [11], ENDSGs have a second semi-functional G-group sampling algorithm $\widetilde{\mathsf{SampG}}$ as well as a second nontrivial H-element in sp (i.e., $\widetilde{h}$). Further, we omit the SampGT-algorithm. Concerning the ENDSG properties, we extend the NDSG properties and assumptions appropriately and introduce one additional assumption (i.e., LS2).

4 An (almost) tightly (μ, q)-IBE-IND-CPA-secure IBE

A variant of the IBE of Chen and Wee [11]. We are now ready to present our variant of Chen and Wee's IBE scheme [11]. As a basic building block we use an ENDSG $\mathsf{ENDSG} = (\mathsf{SampP}, \mathsf{SampG}, \mathsf{SampH}, \widehat{\mathsf{SampG}}, \widetilde{\mathsf{SampG}})$ from Section 3. Besides, for groups G_T (defined below), let $\mathcal{UH}$ be a family of universal hash functions $\mathsf{H} : G_T \to \{0,1\}^k$ such that for any nontrivial subgroup $G'_T \subset G_T$, and for $\mathsf{H} \leftarrow \mathcal{UH}$, $X \leftarrow G'_T$, and $U \leftarrow \{0,1\}^k$, we have $\mathsf{SD}\left((\mathsf{H}, \mathsf{H}(X)); (\mathsf{H}, U)\right) = \mathbf{O}(2^{-k})$. Let $\mathsf{IBE} = (\mathsf{Par}, \mathsf{Gen}, \mathsf{Ext}, \mathsf{Enc}, \mathsf{Dec})$ with identity space $\mathcal{ID} = \{0,1\}^n$, for $n = n(k)$, and message space $\mathcal{M} = \{0,1\}^k$ be defined as follows:

Parameter generation. $\mathsf{Par}(k, n)$ samples $(pp', sp') \leftarrow \mathsf{SampP}(k, 2n)$, for $pp' = (G, H, G_T, N, g, h, e, m, 2n, pars)$ and $sp' = (\widehat{h}, \widetilde{h}, \widehat{pars}, \widetilde{pars})$, and $\mathsf{H} \leftarrow \mathcal{UH}$, and then outputs the public and secret parameters (pp, sp), where $pp = (pp', \mathsf{H})$ and $sp = sp'$.

Key generation. $\mathsf{Gen}(pp, sp)$, given parameters pp and sp, samples $msk \leftarrow H$, and outputs a master public key $mpk := (pp, m(msk))$ and a master secret key msk.

Secret-key extraction. $\mathsf{Ext}(msk, id)$, given $msk \in H$ and an identity $id = (id_1 \ldots id_n) \in \mathcal{ID}$, samples $(h_0, \ldots, h_{2n}) \leftarrow \mathsf{SampH}(pp)$ and outputs a user secret key

$$usk_{id} := (h_0, msk \cdot \prod_{i=1}^{n} h_{2i-id_i}).$$

Encryption. $\mathsf{Enc}(mpk, id, M)$, given $mpk = (pp, m(msk))$, an identity $id = (id_1 \ldots id_n) \in \mathcal{ID}$, and a message $M \in \mathcal{M}$, computes $(g_0, \ldots, g_{2n}) := \mathsf{SampG}(pp; s)$, for $s \leftarrow \mathbb{Z}^*_N$, and $g_T := m(msk)^s$ $(= e(g_0, msk))$, and outputs a ciphertext

$$C_{id} := (g_0, \prod_{i=1}^{n} g_{2i-id_i}, \mathsf{H}(g_T) \oplus M).$$

Decryption. $\mathsf{Dec}(usk_{id}, C_{id'})$, given a user secret key $usk_{id} =: (K_0, K_1)$ and a ciphertext $C_{id'} =: (C_0, C_1, C_2)$, outputs

$$M := \mathsf{H}\left(\frac{e(C_0, K_1)}{e(C_1, K_0)}\right) \oplus C_2.$$

Correctness of IBE. We have

$$\mathsf{H}\left(\frac{e(C_0, K_1)}{e(C_1, K_0)}\right) \oplus C_2 = \mathsf{H}\left(\frac{e(g_0, msk \cdot \prod_{i=1}^{n} h_{2i-id_i})}{e(\prod_{i=1}^{n} g_{2i-id'_i}, h_0)}\right) \oplus \mathsf{H}(g_T) \oplus M \overset{(*)}{=} \mathsf{H}(g_T) \oplus \mathsf{H}(g_T) \oplus M,$$

for $id = id'$. $(*)$ holds due to ENDSG's associativity and projective properties.

(μ, q)-IBE-IND-CPA security of IBE. We base our high-level proof strategy on the IBE-IND-CPA proof strategy of Chen and Wee [11], but deviate on the low level. First, we define auxiliary secret-key extraction $\overline{\mathsf{Ext}}$ and auxiliary encryption $\overline{\mathsf{Enc}}$, random functions $\widehat{\mathsf{R}}_{j,i}$ and $\widetilde{\mathsf{R}}_{j,i}$, pseudo-normal ciphertexts, semi-functional type-$(\cdot, i)$ ciphertexts, and semi-functional type-i user secret keys similarly to [11]:

Auxiliary secret-key extraction. $\overline{\mathsf{Ext}}(pp, msk, id; \mathbf{h})$, given parameter pp, master secret key msk, an identity $id = id_1 \dots id_n \in \mathcal{ID}$, and $\mathbf{h} = (h_0, \dots, h_{2n}) \in (H)^{2n+1}$, outputs a user secret key

$$usk_{id} := (h_0, msk \cdot \prod_{i=1}^{n} h_{2i-id_i}).$$

Auxiliary encryption function. $\overline{\mathsf{Enc}}(pp, id, M; msk, \mathbf{g})$, given parameter pp, identity $id = id_1 \dots id_n \in \mathcal{ID}$, message $M \in \mathcal{M}$, master secret key msk, and $\mathbf{g} = (g_0, \dots, g_{2n}) \in (G)^{2n+1}$, outputs a ciphertext

$$C_{id} := (g_0, \prod_{i=1}^{n} g_{2i-id_i}, \mathsf{H}(e(g_0, msk)) \oplus M).$$

Random function families. Let $id|_i := id_1 \dots id_i$ be the i-bit prefix of an identity id, and let $\mathcal{ID}|_i := \{0,1\}^i$. For an instance j and $i \in [n] \cup \{0\}$, consider functions $\widehat{\mathsf{R}}_{j,i} : \mathcal{ID}|_i \to H$, $id|_i \mapsto (\widehat{h})^{\widehat{\gamma}_{j,i}(id|_i)}$ and $\widetilde{\mathsf{R}}_{j,i} : \mathcal{ID}|_i \to H$, $id|_i \mapsto (\widetilde{h})^{\widetilde{\gamma}_{j,i}(id|_i)}$, where $\widehat{\gamma}_{j,i} : \mathcal{ID}|_i \to \mathbb{Z}^*_{\mathsf{ord}(H)}$, $id|_i \mapsto \widehat{\gamma}_{j,id|_i}$ and $\widetilde{\gamma}_{j,i} : \mathcal{ID}|_i \to \mathbb{Z}^*_{\mathsf{ord}(H)}$, $id|_i \mapsto \widetilde{\gamma}_{j,id|_i}$ are independently and truly random.

Pseudo-normal ciphertexts. Pseudo-normal ciphertexts are generated as

$$\begin{aligned} C_{id} &:= \overline{\mathsf{Enc}}(pp, id, M; msk, \mathbf{g}\widehat{\mathbf{g}}) \\ &= (g_0\widehat{g}_0, \prod_{i=1}^{n} g_{2i-id_i}\widehat{g}_{2i-id_i}, \mathsf{H}(e(g_0\widehat{g}_0, msk)) \oplus M), \end{aligned}$$

for uniform $\mathbf{g} = (g_0, \dots, g_{2n}) \leftarrow \mathsf{SampG}(pp)$ and $\widehat{\mathbf{g}} = (\widehat{g}_0, \dots, \widehat{g}_{2n}) \leftarrow \widehat{\mathsf{SampG}}(pp, sp)$. (Hence, pseudo-normal ciphertexts have G-components sampled from $\widehat{\mathsf{SampG}}$.)

Semi-functional type-$(\wedge, i)$ and type-$(\sim, i)$ ciphertexts. Let $\widehat{\mathsf{R}}_{j,i}$ and $\widetilde{\mathsf{R}}_{j,i}$ be random functions as defined above. Semi-functional ciphertexts of type $(\wedge, i)$ are generated as

$$\begin{aligned} \widehat{C}_{id} &:= \overline{\mathsf{Enc}}(pp, id, M; msk \cdot \widehat{\mathsf{R}}_{j,i}(id|_i) \cdot \widetilde{\mathsf{R}}_{j,i}(id|_i), \mathbf{g}\widehat{\mathbf{g}}) \\ &\overset{(1)}{=} (g_0\widehat{g}_0, \prod_{i=1}^{n} g_{2i-id_i}\widehat{g}_{2i-id_i}, \mathsf{H}(e(g_0\widehat{g}_0, msk \cdot \widehat{\mathsf{R}}_{j,i}(id|_i))) \oplus M) \end{aligned}$$

while semi-functional ciphertexts of type $(\sim, i)$ are generated as

$$\begin{aligned}\widetilde{C}_{id} &:= \overline{\mathsf{Enc}}(pp, id, M; msk \cdot \widehat{\mathsf{R}}_{j,i}(id|_i) \cdot \widetilde{\mathsf{R}}_{j,i}(id|_i), \mathbf{g}\widetilde{\mathbf{g}}) \\ &\overset{(2)}{=} (g_0\widetilde{g}_0, \prod_{i=1}^{n} g_{2i-id_i}\widetilde{g}_{2i-id_i}, \mathsf{H}(e(g_0\widetilde{g}_0, msk \cdot \widetilde{\mathsf{R}}_{j,i}(id|_i))) \oplus M),\end{aligned}$$

where $\mathbf{g} = (g_0, \ldots, g_{2n}) \leftarrow \mathsf{SampG}(pp)$, $\widehat{\mathbf{g}} = (\widehat{g}_0, \ldots, \widehat{g}_{2n}) \leftarrow \widehat{\mathsf{SampG}}(pp)$, and $\widetilde{\mathbf{g}} = (\widetilde{g}_0, \ldots, \widetilde{g}_{2n}) \leftarrow \widetilde{\mathsf{SampG}}(pp)$, while (1) and (2) hold due to ENDSG's properties.

Semi-functional type-i user secret keys. Let $\widehat{\mathsf{R}}_{j,i}$ and $\widetilde{\mathsf{R}}_{j,i}$ be defined as above. For $\mathbf{h} = (h_0, \ldots, h_{2n}) \leftarrow \mathsf{SampH}(pp)$, semi-functional type-$i$ user secret keys are generated as

$$\begin{aligned}usk_{id} &:= \overline{\mathsf{Ext}}(pp, msk \cdot \widehat{\mathsf{R}}_{j,i}(id|_i) \cdot \widetilde{\mathsf{R}}_{j,i}(id|_i), id; \mathbf{h}) \\ &= (h_0, msk \cdot \widehat{\mathsf{R}}_{j,i}(id|_i) \cdot \widetilde{\mathsf{R}}_{j,i}(id|_i) \cdot \prod_{i=1}^{n} h_{2i-id_i}).\end{aligned}$$

Theorem 4.1. *If* ENDSG *is an ENDSG system as defined in Section 3 and* H *is a universal hash function, then* IBE *defined as above is weakly (μ, q)-IBE-IND-CPA-secure. Concretely, for any weak PPT adversary A with at most $q' = q'(k)$ key extraction queries per instance and running time t in the (μ, q)-IBE-IND-CPA security experiment with* IBE*, there are distinguishers D_1 on LS1, D_2 on LS2, and D_3 on NH with running times $t'_1 \approx t'_2 \approx t'_3 \approx t + \mathbf{O}(\mu n k^c (q + q'))$, respectively, for some constant $c \in \mathbb{N}$, with*

$$\begin{aligned}\mathsf{Adv}^{(\mu,q)\text{-ibe-ind-cpa}}_{\mathsf{IBE},A}(k, n) \leq\ & \mathsf{Adv}^{\mathrm{ls1}}_{\mathsf{ENDSG},\mathsf{G},D_1}(k, 2n) + 2n \cdot \mathsf{Adv}^{\mathrm{ls2}}_{\mathsf{ENDSG},\mathsf{G},D_2}(k, 2n) \\ &+ n \cdot \mathsf{Adv}^{\mathrm{nh}}_{\mathsf{ENDSG},\mathsf{G},D_3}(k, 2n, \mu q') + \mu q \cdot \mathbf{O}(2^{-k}), \qquad (1)\end{aligned}$$

for group generator G *defined as above.*

Proof. We show the (μ, q)-IBE-IND-CPA security of IBE for any weak PPT adversary A in a sequence of games where we successively change the games until we arrive at a game where A has only negligible advantage (i.e., success probability of $1/2$) in the sense of (μ, q)-IBE-IND-CPA. Let $S_{A,j}$ be the event that A succeeds in Game j. We give an overview how the challenge ciphertexts and user secret keys are generated in Table 1.

Game 0. Game 0 is the (μ, q)-IBE-IND-CPA experiment as defined above.

Game 1. Game 1 is defined as Game 0 apart from the fact that all challenge ciphertexts are pseudo-normal.

Game 2.i.0. Game $2.i.0$ is defined as Game 1 except that all user secret keys are semi-functional of type $(i-1)$ and all challenge ciphertexts are semi-functional of type-$(\wedge, i-1)$, for all $i \in [n]$.

Game 2.i.1. Game $2.i.1$ is defined as Game $2.i.0$ except that if and only if the i-th bit of a challenge identity is 1, then the corresponding challenge ciphertext is semi-functional of type $(\sim, i-1)$. (Otherwise, if and only if the i-th bit of a challenge identity is 0, then the corresponding challenge ciphertext is semi-functional of type $(\wedge, i-1)$.)

Game 2.i.2. Game $2.i.2$ is defined as Game $2.i.1$ except that the challenge ciphertexts are semi-functional of type $(\cdot, i)$ (where $\cdot$ can be $\wedge$ or $\sim$ as defined in Game $2.i.1$, i.e., depending on the i-th challenge identity bit) and the user secret keys are semi-functional of type i.

Game 3. Game 3 is defined as Game $2.n.0$ except that the challenge ciphertexts are semi-functional of type $(\wedge, n)$ and the user secret keys are semi-functional of type n.

Game	Challenge ciphertexts for $id^*_{j,i'}$	User secret keys for id
G. 0	$\mathsf{Enc}(mpk_j, id^*_{j,i'}, M^*_{j,i',b})$	$\mathsf{Ext}(msk_j, id)$
G. 1	$\overline{\mathsf{Enc}}(pp, id^*_{j,i'}, M^*_{j,i',b}; msk_j, \mathbf{g}\widehat{\mathbf{g}})$	$\overline{\mathsf{Ext}}(pp, msk_j, id; \mathbf{h})$
G. 2.i.0	$\overline{\mathsf{Enc}}(pp, id^*_{j,i'}, M^*_{j,i',b}; msk_j \cdot \widehat{\mathsf{R}}_{j,i-1}(id^*_{j,i'}\|_{i-1}), \mathbf{g}\widehat{\mathbf{g}})$	$\overline{\mathsf{Ext}}(pp, msk_j \cdot \widehat{\mathsf{R}}_{j,i-1}(id\|_{i-1}) \cdot \widetilde{\mathsf{R}}_{j,i-1}(id\|_{i-1}), id; \mathbf{h})$
G. 2.i.1	if $id^*_{j,i',i} = 0$: $\overline{\mathsf{Enc}}(pp, id^*_{j,i'}, M^*_{j,i',b}; msk_j \cdot \widehat{\mathsf{R}}_{j,i-1}(id^*_{j,i'}\|_{i-1}), \mathbf{g}\widehat{\mathbf{g}})$ if $id^*_{j,i',i} = 1$: $\overline{\mathsf{Enc}}(pp, id^*_{j,i'}, M^*_{j,i',b}; msk_j \cdot \widetilde{\mathsf{R}}_{j,i-1}(id^*_{j,i'}\|_{i-1}), \mathbf{g}\widetilde{\mathbf{g}})$	$\overline{\mathsf{Ext}}(pp, msk_j \cdot \widehat{\mathsf{R}}_{j,i-1}(id\|_{i-1}) \cdot \widetilde{\mathsf{R}}_{j,i-1}(id\|_{i-1}), id; \mathbf{h})$
G. 2.i.2	if $id^*_{j,i',i} = 0$: $\overline{\mathsf{Enc}}(pp, id^*_{j,i'}, M^*_{j,i',b}; msk_j \cdot \widehat{\mathsf{R}}_{j,i}(id^*_{j,i'}\|_i), \mathbf{g}\widehat{\mathbf{g}})$ if $id^*_{j,i',i} = 1$: $\overline{\mathsf{Enc}}(pp, id^*_{j,i'}, M^*_{j,i',b}; msk_j \cdot \widetilde{\mathsf{R}}_{j,i}(id^*_{j,i'}\|_i), \mathbf{g}\widetilde{\mathbf{g}})$	$\overline{\mathsf{Ext}}(pp, msk_j \cdot \widehat{\mathsf{R}}_{j,i}(id\|_i) \cdot \widetilde{\mathsf{R}}_{j,i}(id\|_i), id; \mathbf{h})$
G. 3	$\overline{\mathsf{Enc}}(pp, id^*_{j,i'}, M^*_{j,i',b}; msk_j \cdot \widehat{\mathsf{R}}_{j,n}(id^*_{j,i'}), \mathbf{g}\widehat{\mathbf{g}})$	$\overline{\mathsf{Ext}}(pp, msk_j \cdot \widehat{\mathsf{R}}_{j,n}(id) \cdot \widetilde{\mathsf{R}}_{j,n}(id), id; \mathbf{h})$
G. 4	$\overline{\mathsf{Enc}}(pp, id^*_{j,i'}, R_{j,i'}; msk_j \cdot \widehat{\mathsf{R}}_{j,n}(id^*_{j,i'}), \mathbf{g}\widehat{\mathbf{g}})$	$\overline{\mathsf{Ext}}(pp, msk_j \cdot \widehat{\mathsf{R}}_{j,n}(id) \cdot \widetilde{\mathsf{R}}_{j,n}(id), id; \mathbf{h})$

Table 1: Instance-j challenge ciphertexts for challenge identity $id^*_{j,i'}$, for $\mathbf{g} \leftarrow \mathsf{SampG}(pp)$, for $\widehat{\mathbf{g}} \leftarrow \widehat{\mathsf{SampG}}(pp, sp)$, for $\widetilde{\mathbf{g}} \leftarrow \widetilde{\mathsf{SampG}}(pp, sp)$, for $R_{j,i'} \leftarrow \{0,1\}^k$, and for instance-$j$ user secret keys for identity id, for $\mathbf{h} \leftarrow \mathsf{SampH}(pp)$, for all $(j, i', i) \in [\mu] \times [q] \times [n]$. The differences between games are given by underlining.

Game 4. Game 4 is defined as Game 3 except that the challenge ciphertext messages are uniform k-length bitstrings.

Lemma 4.2 (Game 0 to Game 1). *If the G- and H-subgroups property and LS1 of* ENDSG *hold, Game 0 and Game 1 are computationally indistinguishable. Concretely, for any PPT adversary A with at most $q' = q'(k)$ extraction queries per instance and running time t in the (μ, q)-IBE-IND-CPA security experiment with* IBE *there is a distinguisher D on LS1 with running time $t' \approx t + \mathbf{O}(\mu n k^c (q + q'))$, for some constant $c \in \mathbb{N}$, such that*

$$|\Pr[S_{A,0}] - \Pr[S_{A,1}]| \leq \mathsf{Adv}^{\mathrm{ls1}}_{\mathsf{ENDSG},\mathsf{G},D}(k, 2n). \tag{2}$$

Proof. In Game 0, all challenge ciphertexts are normal in the sense of IBE while in Game 1, all challenge ciphertexts are pseudo-normal. In the following, we give a description and its analysis of a LS1 distinguisher that uses any efficient IBE-attacker in the (μ, q)-IBE-IND-CPA sense.

Description. The challenge input is provided as $(pp, \mathbf{T})$, where $\mathbf{T}$ is either $\mathbf{g}$ or $\mathbf{g}\widehat{\mathbf{g}}$, for $pp = (G, H, G_T, N, g, h, e, m, 2n, pars)$, $\mathbf{g} \leftarrow \mathsf{SampG}(pp)$, and $\widehat{\mathbf{g}} \leftarrow \widehat{\mathsf{SampG}}(pp, sp)$. First, D samples $(msk_j)_j \leftarrow (H)^\mu$, sets $mpk_j := (pp, \mathsf{H}, m(msk_j))$, for all j, for $\mathsf{H} \leftarrow \mathcal{UH}$, and sends $(mpk_j)_j$ to A. During the experiment, D answers instance-j secret key extraction queries to oracle $\mathsf{Ext}(msk_j, \cdot)$, for $id \in \mathcal{ID}$, as

$$\overline{\mathsf{Ext}}(pp, msk_j, id; \mathsf{SampH}(pp)),$$

for all j. (We assume that A queries at most q' user secret keys per instance.) Then, D fixes a bit $b \leftarrow \{0,1\}$. A may adaptively query its Enc'-oracle; for A-chosen instance-j challenge identity $id^*_{j,i} \in \mathcal{ID}$ and equal-length messages $(M^*_{j,i,0}, M^*_{j,i,1})$. D returns

$$\overline{\mathsf{Enc}}(pp, id^*_{j,i}, M^*_{j,i,b}; msk_j, \mathbf{T}^{s_{j,i}})$$

to A, for $s_{j,i} \leftarrow \mathbb{Z}^*_N$, for all $(j, i) \in [\mu] \times [q]$. (We assume that A queries at most q challenge ciphertexts per instance.) Eventually, A outputs a guess b'. D outputs 1 if $b' = b$ and A is valid in the sense of (μ, q)-IBE-IND-CPA, else outputs 0.

Analysis. The provided master public keys and the A-requested user secret keys yield the correct distribution and are consistent in the sense of Game 0 and Game 1. Due to ENDSG's G- and H-subgroups property, we have that $\mathbf{T}$ is uniformly distributed over the generators of a nontrivial subgroup of G^{2n+1}. Hence, $\mathbf{T}^s$, for $s \leftarrow \mathbb{Z}_N^*$, is distributed uniformly over the generators of a nontrivial subgroup of G^{2n+1} and, thus, all challenge ciphertexts yield the correct distribution in the sense of Game 0 and Game 1. If $\mathbf{T} = \mathbf{g}$, then the challenge ciphertexts are distributed identically as in Game 0. Otherwise, i.e., if $\mathbf{T} = \mathbf{g}\widehat{\mathbf{g}}$, then the challenge ciphertexts are distributed identically as in Game 1. Hence, (2) follows. □

Lemma 4.3 (**Game 1 to Game 2.1.0**). *If the orthogonality property of* ENDSG *holds, the output distributions of Game 1 and Game 2.1.0 are the same. Concretely, for any PPT adversary A in the (μ, q)-IBE-IND-CPA security experiment with* IBE*, it holds that*

$$\Pr[S_{A,1}] = \Pr[S_{A,2.1.0}]. \tag{3}$$

Proof. In this bridging step, we argue that each instance-j master secret key msk_j, with $msk_j \leftarrow H$, generated as in Game 1 and the (implicit) instance-j master secret keys msk'_j, with $msk'_j := msk''_j \cdot \widehat{\mathsf{R}}_{j,0}(\varepsilon) \cdot \widetilde{\mathsf{R}}_{j,0}(\varepsilon)$, for $msk''_j \leftarrow H$ and $\widehat{\mathsf{R}}_{j,0}, \widetilde{\mathsf{R}}_{j,0}$ defined as above, generated as in Game 2.1.0, are identically distributed, for all j. Note that the master public keys for A contain $(m(msk_j))_j$; but since $((m(msk'_j))_j = (m(msk''_j))_j$, which is due to the orthogonality property of ENDSG, no $\widehat{\mathsf{R}}_{j,0}$-information and no $\widetilde{\mathsf{R}}_{j,0}$-information is given out in the master public keys. Further, since $(msk_j)_j$ and $(msk''_j)_j$ are identically distributed, it follows that (3) holds. □

Lemma 4.4 (**Game 2.i.0 to Game 2.i.1**). *If the G- and H-subgroups property and LS2 of* ENDSG *hold, Game 2.i.0 and Game 2.i.1 are computationally indistinguishable. Concretely, for any PPT adversary A with at most $q' = q'(k)$ extraction queries per instance and running time t in the (μ, q)-IBE-IND-CPA security experiment with* IBE*, there is a distinguisher D on LS2 with running time $t' \approx t + \mathbf{O}(\mu n k^c (q + q'))$, for some constant $c \in \mathbb{N}$, such that*

$$|\Pr[S_{2.i.0}] - \Pr[S_{2.i.1}]| \leq \mathsf{Adv}^{\mathrm{ls2}}_{\mathsf{ENDSG},\mathsf{G},D}(k, 2n), \tag{4}$$

for all $i \in [n]$.

Proof. In Game 2.i.0, we have semi-functional type-$(\wedge, i-1)$ challenge ciphertexts while in Game 2.i.1, challenge ciphertexts are semi-functional of type $(\sim, i-1)$ if and only if the i-th challenge identity bit is 1.

Description. The challenge input is provided as $(pp, \widehat{h}\widetilde{h}, \mathbf{g}'\widehat{\mathbf{g}}', \mathbf{T})$, where $\mathbf{T}$ is either $\mathbf{g}\widehat{\mathbf{g}}$ or $\mathbf{g}\widetilde{\mathbf{g}}$, for pp as before, for $\widehat{h}, \widetilde{h}$ specified in sp, for $\mathbf{g}, \mathbf{g}' \leftarrow \mathsf{SampG}(pp)$, $\widehat{\mathbf{g}}, \widehat{\mathbf{g}}' \leftarrow \widehat{\mathsf{SampG}}(pp, sp)$, and $\widetilde{\mathbf{g}} \leftarrow \widetilde{\mathsf{SampG}}(pp, sp)$. First, D samples $(msk_j)_j \leftarrow (H)^\mu$, sets $mpk_j := (pp, \mathsf{H}, m(msk_j))$, for all j, for $\mathsf{H} \leftarrow \mathcal{UH}$, for m specified in pp, and sends $(mpk_j)_j$ to A. Further, D defines a truly random function $\mathsf{R} : [\mu] \times \{0,1\}^{i-1} \to \langle \widehat{h}\widetilde{h} \rangle$. During the experiment, D answers instance-j secret key extraction queries to oracle $\mathsf{Ext}(msk_j, \cdot)$ as

$$\overline{\mathsf{Ext}}(pp, msk_j \cdot \mathsf{R}(j, id|_{i-1}), id; \mathsf{SampH}(pp)),$$

for $id \in \mathcal{ID}$ and all j. (Again, we assume that A queries at most q' user secret keys per instance and we set $id|_0 = \{0,1\}^0 =: \varepsilon$.) A may adaptively query its Enc'-oracle; for instance-j challenge identity $id^*_{j,i'} = id^*_{j,i',1} \ldots, id^*_{j,i',n} \in \mathcal{ID}$ and equal-length messages $(M^*_{j,i',0}, M^*_{j,i',1})$, D returns

$$\overline{\mathsf{Enc}}(pp, id^*_{j,i'}, M^*_{j,i',b}; msk_j \cdot \mathsf{R}(j, id^*_{j,i'}|_{i-1}), (\mathbf{g}'\widehat{\mathbf{g}}')^{s_{j,i'}}) \quad \text{if } id^*_{j,i',i} = 0,$$

$$\overline{\mathsf{Enc}}(pp, id^*_{j,i'}, M^*_{j,i',b}; msk_j \cdot \mathsf{R}(j, id^*_{j,i'}|_{i-1}), \mathbf{T}^{s_{j,i'}}) \quad \text{if } id^*_{j,i',i} = 1,$$

to A, for $b \leftarrow \{0,1\}$, for $s_{j,i'} \leftarrow \mathbb{Z}_N^*$, for all $(j,i') \in [\mu] \times [q]$. Eventually, A outputs a guess b'. D outputs 1 if $b' = b$ and A is valid in the sense of (μ,q)-IBE-IND-CPA, else outputs 0.

Analysis. The master public keys yield the correct distribution as well as the requested user secret keys (which is due to ENDSG's G- and H-subgroups property, i.e., the output of SampH is uniformly distributed over the generators of a nontrivial subgroup of H^{2n+1}). For the challenge ciphertexts, note that $\mathbf{g}'\widehat{\mathbf{g}}'$ and $\mathbf{T}$ are uniformly distributed over the generators of their respective nontrivial subgroup of G^{2n+1} and, hence, $(\mathbf{g}'\widehat{\mathbf{g}}')^s$ and $\mathbf{T}^s$, for $s \leftarrow \mathbb{Z}_N^*$, are distributed uniformly over the generators of their respective nontrivial G^{2n+1}-subgroup as well. If $\mathbf{T} = \mathbf{g}\widehat{\mathbf{g}}$, then the challenge ciphertexts are distributed identically as in Game $2.i.0$. Otherwise, if $\mathbf{T} = \mathbf{g}\widetilde{\mathbf{g}}$, then the challenge ciphertexts are distributed identically as in Game $2.i.1$ (where, in both cases, ENDSG's orthogonality and non-degeneracy properties hold; thus, $\widehat{h}$ and $\widetilde{h}$ must contain coprime nontrivial elements and the challenge ciphertexts yield the correct distribution). Hence, (4) follows. □

Lemma 4.5 (Game 2.i.1 to Game 2.i.2). *If the G- and H-subgroups property and NH of* ENDSG *hold, Game 2.i.1 and Game 2.i.2 are computationally indistinguishable. Concretely, for any PPT adversary A with at most $q' = q'(k)$ extraction queries per instance and running time t in the (μ,q)-IBE-IND-CPA security experiment with* IBE*, there is a distinguisher D on NH with running time $t' \approx t + \mathbf{O}(\mu n k^c (q+q'))$, for some constant $c \in \mathbb{N}$, such that*

$$|\Pr[S_{2.i.1}] - \Pr[S_{2.i.2}]| \leq \mathsf{Adv}^{\mathrm{nh}}_{\mathsf{ENDSG},\mathsf{G},D}(k, 2n, \mu q'), \tag{5}$$

for all $i \in [n]$.

Proof. In Game $2.i.1$, the challenge ciphertexts are semi-functional of type $(\wedge, i-1)$ if the i-th bit of the challenge identity is 0 and semi-functional of type $(\sim, i-1)$ if the i-th bit of the challenge identity is 1, while in Game $2.i.2$, all challenge ciphertexts are of type $(\cdot, i)$.

Description. The challenge input is $(pp, \widehat{h}, \widetilde{h}, \widehat{\mathbf{g}}_{-(2i-1)}, \widetilde{\mathbf{g}}_{-2i}, (\mathbf{T}_{1,1}, \ldots, \mathbf{T}_{\mu,q'}))$, where $\mathbf{T}_{j,i'}$ equals either

$$(h_{j,i',0}, \ldots, h_{j,i',2n}) \quad \text{or} \quad (h_{j,i',0}, \ldots, h_{j,i',2i-1} \cdot (\widehat{h})^{\widehat{\gamma}_{j,i'}}, h_{j,i',2i} \cdot (\widetilde{h})^{\widetilde{\gamma}_{j,i'}}, \ldots, h_{j,i',2n}),$$

for pp as before, $\widehat{h}, \widetilde{h}$ specified as in sp, for $\widehat{\mathbf{g}} \leftarrow \widehat{\mathsf{SampG}}(pp, sp)$, for $\widetilde{\mathbf{g}} \leftarrow \widetilde{\mathsf{SampG}}(pp, sp)$, for $(h_{j,i',0}, \ldots, h_{j,i',2n}) \leftarrow \mathsf{SampH}(pp)$, and for uniform $\widehat{\gamma}_{j,i'}, \widetilde{\gamma}_{j,i'} \leftarrow \mathbb{Z}^*_{\mathsf{ord}(H)}$, for all $(j,i') \in [\mu] \times [q']$. D samples $(msk_j)_j \leftarrow (H)^\mu$, sets $mpk_j := (pp, \mathsf{H}, m(msk_j))$, for all j, for $\mathsf{H} \leftarrow \mathcal{UH}$, for m specified in pp, and sends $(mpk_j)_j$ to A. Further, D defines random functions $\widehat{\mathsf{R}}_{j,i-1}, \widetilde{\mathsf{R}}_{j,i-1}$ as above. In addition, for identity $id = id_1 \ldots id_n \in \mathcal{ID}$, we will define

$$\begin{aligned}
&\widehat{\mathsf{R}}_{j,i}(id|_i) := \widehat{\mathsf{R}}_{j,i-1}(id|_{i-1}) \quad \text{and (implicitly)} \quad \widetilde{\mathsf{R}}_{j,i}(id|_i) := \widetilde{\mathsf{R}}_{j,i-1}(id|_{i-1}) \cdot (\widetilde{h})^{\widetilde{\gamma}_{j,i'}} \quad \text{if } id_i = 0,\\
&\widetilde{\mathsf{R}}_{j,i}(id|_i) := \widetilde{\mathsf{R}}_{j,i-1}(id|_{i-1}) \quad \text{and (implicitly)} \quad \widehat{\mathsf{R}}_{j,i}(id|_i) := \widehat{\mathsf{R}}_{j,i-1}(id|_{i-1}) \cdot (\widehat{h})^{\widehat{\gamma}_{j,i'}} \quad \text{if } id_i = 1,
\end{aligned}$$

for suitable $(j,i') \in [\mu] \times [q']$ as shown below. Further, during the experiment, D returns the i'-th secret key extraction query in instance j for an identity id, with prefix $id|_i$ not a prefix of an already queried identity in instance j, as

$$\begin{aligned}
&\overline{\mathsf{Ext}}(pp, msk_j \cdot \widehat{\mathsf{R}}_{j,i}(id|_i) \cdot \widetilde{\mathsf{R}}_{j,i-1}(id|_{i-1}), id; \mathbf{T}_{j,i'}) \quad \text{if } id_i = 0,\\
&\overline{\mathsf{Ext}}(pp, msk_j \cdot \widehat{\mathsf{R}}_{j,i-1}(id|_{i-1}) \cdot \widetilde{\mathsf{R}}_{j,i}(id|_i), id; \mathbf{T}_{j,i'}) \quad \text{if } id_i = 1,
\end{aligned}$$

for all (j,i'). (Note that $id|_i$ could be a valid prefix in any other instance different to j. Further, we assume that A queries at most q' user secret keys per instance.) For an identity prefixes $id|_i$

that is a prefix of an already queried identity in instance j, let $(j, i'') \in [\mu] \times [q']$ be the index of that query. In that case, D returns

$$\begin{aligned}
&\overline{\mathsf{Ext}}(pp, msk_j \cdot \widehat{\mathsf{R}}_{j,i}(id|_i) \cdot \widetilde{\mathsf{R}}_{j,i-1}(id|_{i-1}), id; \mathbf{T}_{j,i''} \cdot \mathsf{SampH}(pp)) \quad \text{if } id_i = 0,\\
&\overline{\mathsf{Ext}}(pp, msk_j \cdot \widehat{\mathsf{R}}_{j,i-1}(id|_{i-1}) \cdot \widetilde{\mathsf{R}}_{j,i}(id|_i), id; \mathbf{T}_{j,i''} \cdot \mathsf{SampH}(pp)) \quad \text{if } id_i = 1,
\end{aligned}$$

for all j. (Note that we use SampH to rerandomize the H^{2n+1}-subgroup element of $\mathbf{T}_{j,i''}$.) Further, A may adaptively query its Enc'-oracle; for A-chosen instance-j challenge identity $id^*_{j,i'''} = id^*_{j,i''',1} \ldots, id^*_{j,i''',n} \in \mathcal{ID}$ and equal-length messages $(M^*_{j,i''',0}, M^*_{j,i''',1})$ and returns

$$\overline{\mathsf{Enc}}(pp, id^*_{j,i'''}, M^*_{j,i''',b}; msk_j \cdot \widehat{\mathsf{R}}_{j,i}(id^*_{j,i'''}|_i), (\mathbf{g}_{-(2i-1)}\widehat{\mathbf{g}}_{-(2i-1)})^{s_{j,i'''}}) \text{ if } id^*_{j,i''',i} = 0,$$

$$\overline{\mathsf{Enc}}(pp, id^*_{j,i'''}, M^*_{j,i''',b}; msk_j \cdot \widetilde{\mathsf{R}}_{j,i}(id^*_{j,i'''}|_i), (\mathbf{g}_{-2i}\widetilde{\mathbf{g}}_{-2i})^{s_{j,i'''}}) \text{ if } id^*_{j,i''',i} = 1,$$

to A, for $s_{j,i'''} \leftarrow \mathbb{Z}^*_N$, for $\mathbf{g} \leftarrow \mathsf{SampG}(pp)$, for fixed $b \leftarrow \{0,1\}$, for all (j, i'''). (Note that a modified $\overline{\mathsf{Enc}}$-input is provided with only $4n$ instead of $4n+2$ elements. Nevertheless, the omitted elements are not needed to generate a valid ciphertext (since it is consistent with the challenge identities $(id^*_{j,i'''})_{j,i'''}$). Hence, we assume that $\overline{\mathsf{Enc}}$ works as desired.) Eventually, A outputs a guess b'. D outputs 1 if $b' = b$ and A is valid in the sense of (μ, q)-IBE-IND-CPA, else outputs 0.

Analysis. Note that the provided master public keys yield the correct distribution. For the A-requested user secret keys, we have that since $\widehat{h}$ and $\widetilde{h}$ have nontrivial H-elements of coprime order (again, this is due to ENDSG's orthogonality and non-degeneracy properties), the random functions $\widehat{\mathsf{R}}_{j,i-1}, \widehat{\mathsf{R}}_{j,i}$ and $\widetilde{\mathsf{R}}_{j,i-1}, \widetilde{\mathsf{R}}_{j,i}$ yield the correct distributions in the sense of Game 2.i.1 and Game 2.i.2, respectively. Due to the G- and H-subgroups property of ENDSG, $\mathbf{g}_{-(2i-1)}$ and $\widehat{\mathbf{g}}_{-(2i-1)}$ as well as $\mathbf{g}_{-2i}$ and $\widetilde{\mathbf{g}}_{-2i}$ are uniformly distributed over the generators of their respective nontrivial subgroups of G^{2n} and, thus, $(\mathbf{g}_{-(2i-1)}\widehat{\mathbf{g}}_{-(2i-1)})^s$ and $(\mathbf{g}_{-2i}\widetilde{\mathbf{g}}_{-2i})^s$, for $s \leftarrow \mathbb{Z}^*_N$, are distributed uniformly over the generators of their respective nontrivial subgroup of G^{2n}. Further, if $id^*_{j,i''',i} = 0$, then it holds that $\widehat{\mathsf{R}}_{j,i}(id^*_{j,i'''}|_i) = \widehat{\mathsf{R}}_{j,i-1}(id^*_{j,i'''}|_{i-1})$ and all required components $\widehat{\mathbf{g}}_{-(2i-1)}$ to create the challenge ciphertexts are given. Analogously, if $id^*_{j,i''',i} = 1$, then we have $\widetilde{\mathsf{R}}_{j,i}(id^*_{j,i'''}|_i) = \widetilde{\mathsf{R}}_{j,i-1}(id^*_{j,i'''}|_{i-1})$ and all necessary components $\widetilde{\mathbf{g}}_{-2i}$ are provided as needed. Hence, the challenge ciphertexts and user secret keys yield the correct distribution. If $(\mathbf{T}_{j,i'})_{j,i'} = (h_{j,i',0}, \ldots, h_{j,i',2n})_{i'}$, then the user secret keys are distributed identically as in Game 2.i.1. If $(\mathbf{T}_{j,i'})_{j,i'} = (h_{j,i',0}, \ldots, h_{j,i',2i-1} \cdot (\widehat{h})^{\widehat{\gamma}_{j,i'}}, h_{j,i',2i} \cdot (\widetilde{h})^{\widetilde{\gamma}_{j,i'}}, \ldots, h_{j,i',2n})_{j,i'}$, then the user secret keys are distributed identically as in Game 2.i.2. Thus, (5) follows. □

Lemma 4.6 (Game 2.i-1.2 to Game 2.i.0). *If the G- and H-subgroups property and LS2 of* ENDSG *hold, Game 2.i-1.1 and Game 2.i.0 are computationally indistinguishable. Concretely, for any PPT adversary A with at most $q' = q'(k)$ extraction queries per instance and running time t in the (μ, q)-IBE-IND-CPA security experiment with* IBE*, there is a distinguisher D with running time $t' \approx t + \mathbf{O}(\mu n k^c (q + q'))$, for some constant $c \in \mathbb{N}$, such that*

$$|\Pr[S_{2.i-1.2}] - \Pr[S_{2.i.0}]| \leq \mathsf{Adv}^{\mathrm{ls2}}_{\mathsf{ENDSG},\mathsf{G},D}(k, 2n), \tag{6}$$

for all $i \in [n] \setminus \{1\}$.

Proof. In Game 2.$i-1$.2, challenge ciphertexts are of type $(\cdot, i-1)$ and depend on the $(i-1)$-th challenge identity bit while in Game 2.i.0, challenge ciphertexts are of type $(\wedge, i-1)$. This proof is very similar to the proof of Lemma 4.4 except that the challenge ciphertexts depend on the $(i-1)$-th instead of the i-th challenge identity bit. □

Lemma 4.7 (**Game 2.n.2 to Game 3**). *If the G- and H-subgroups property and LS2 of* ENDSG *hold, Game 2.n.2 and Game 3 are computationally indistinguishable. Concretely, for any PPT adversary A with at most $q' = q'(k)$ extraction queries per instance and running time t in the (μ, q)-IBE-IND-CPA security experiment with* IBE*, there is a distinguisher D with running time $t' \approx t + \mathbf{O}(\mu n k^c (q + q'))$, for some constant $c \in \mathbb{N}$, such that*

$$|\Pr[S_{A,2.n.2}] - \Pr[S_{A,3}]| \leq \mathsf{Adv}^{\mathrm{ls2}}_{\mathsf{ENDSG},\mathsf{G},D}(k, 2n). \tag{7}$$

Proof. It is easy to see that Game 3 and a potential Game 2.n+1.0 would be identical. Hence, we can reassemble the proof of Lemma 4.6 with $i := n + 1$ and (7) directly follows. □

Lemma 4.8 (**Game 3 to Game 4, weak adversaries**). *Game 3 and Game 4 are statistically indistinguishable. Concretely, for any PPT weak adversary A on the (μ, q)-IBE-IND-CPA security of* IBE*, it holds that*

$$|\Pr[S_{A,3}] - \Pr[S_{A,4}]| \leq \mu q \cdot \mathbf{O}(2^{-k}). \tag{8}$$

Proof. In Game 4, we replace each challenge message $M_{j,i',b}$, for challenge bit $b \in \{0,1\}$, with a (fresh) uniformly random k-length bitstring $R_{j,i'} \leftarrow \{0,1\}^k$. We argue with ENDSG's non-degeneracy property and the universality of H for this change. Concretely, for instance-j Game-3 challenge ciphertexts

$$\begin{aligned}&\overline{\mathsf{Enc}}(pp, id^*_{j,i'}, M^*_{j,i',b}; msk_j \cdot \widehat{\mathsf{R}}_{j,n}(id^*_{j,i'}), (\mathbf{g}\widehat{\mathbf{g}})^{s_{j,i'}})\\ &= ((g_0\widehat{g}_0)^{s_{j,i'}}, (\prod_{i=1}^{n} g_{2i-id^*_{j,i',i}} \widehat{g}_{2i-id^*_{j,i',i}})^{s_{j,i'}}, \mathsf{H}(e((g_0\widehat{g}_0)^{s_{j,i'}}, msk_j \cdot \widehat{\mathsf{R}}_{j,n}(id^*_{j,i'}))) \oplus M^*_{j,i',b}),\end{aligned}$$

for $\mathbf{g} \leftarrow \mathsf{SampG}(pp)$, for $\widehat{\mathbf{g}} \leftarrow \widehat{\mathsf{SampG}}(pp, sp)$, for $s_{j,i'} \leftarrow \mathbb{Z}^*_N$, for all $i' \in [q]$, note that $e((\widehat{g}_0)^{s_{j,i'}}, \widehat{\mathsf{R}}_{j,n}(id^*_{j,i'})) = e((\widehat{g}_0)^{s_{j,i'}}, \widehat{h})^{\widehat{\gamma}_{j,i'}}$, for uniform $\widehat{\gamma}_{j,i'} \in \mathbb{Z}^*_{\mathsf{ord}(H)}$, is uniformly distributed in a nontrivial subgroup $G'_T \subset G_T$ due to the non-degeneracy property of ENDSG. Furthermore, since A is a *weak* adversary, all the $\widehat{\mathsf{R}}_{j,n}$ are for different preimages and thus independently random. Hence, since H is a (randomly chosen) universal hash function, we have that $\mathsf{SD}((\mathsf{H}, \mathsf{H}(X)); (\mathsf{H}, U)) = \mathbf{O}(2^{-k})$, for $X \leftarrow G'_T$ and $U \leftarrow \{0,1\}^k$. A union bound yields (8). □

Lemma 4.9 (**Game 4**). *For any PPT adversary A in the (μ, q)-IBE-IND-CPA security experiment with* IBE*, it holds that*

$$\Pr[S_{A,4}] = 1/2. \tag{9}$$

Proof. In Game 4, for (uniform) challenge bit $b \in \{0,1\}$, we provide A with challenge ciphertexts that include a uniform k-length bitstring instead of a A-chosen b-dependent message, for each instance and challenge. Hence, b is completely hidden from A and (9) follows. □

Taking (2), (3), (4), (5), (6), (7), (8), and (9) together, shows (1). □

From weak to full (μ, q)-IBE-IND-CPA security. The analysis above shows only weak security: we must assume that the adversary A never asks for encryptions under the same challenge identity and for the same scheme instance twice. We do not know how to remove this restriction assuming only the abstract properties of ENDSGs. However, at the cost of one tight additional reduction to (a slight variant of) the Bilinear Decisional Diffie-Hellman (BDDH) assumption, we can show full (μ, q)-IBE-IND-CPA security.

Concretely, in Game 3, challenge ciphertexts for A are prepared using (the hash value of) $e(\widehat{g}_0^s, \widehat{h}^\gamma)$ as a mask to hide the plaintext behind. Here, $\widehat{g}_0^s$ and $\widehat{h}$ are public (as part of the ciphertext, resp. public parameters), s is a fresh exponent chosen randomly for each

encryption, and γ is a random exponent that however only depends on the scheme instance and identity. (Thus, γ will be reused for different encryptions under the same identity). Hence, if we show that many tuples $(\widehat{g}^{s_i}, e(\widehat{g}_0^{s_i}, \widehat{h}^{\gamma}))$ (for different s_i but the same γ) are computationally indistinguishable from random tuples, we obtain that even multiple encryptions under the same identity hide the plaintexts, and we obtain full security.

Of course, the corresponding reduction should be tight, in the sense that it should not degrade in the number of tuples, or in the number of considered γ.

A (subgroup) variant of the BDDH assumption (s-BDDH). For any PPT adversary D, we have that the function

$$\begin{aligned}\mathsf{Adv}^{\text{s-bddh}}_{\mathsf{ENDSG},\mathsf{G},D}(k,n) := |\Pr\left[D(pp, \mathbf{g}, \mathbf{g}^a, \widehat{\mathbf{g}}, \widehat{\mathbf{g}}^a, \widehat{g}_0^b, \widehat{h}, \widehat{h}^b, \widehat{h}^c, e(\widehat{g}_0, \widehat{h})^{abc}) = 1\right] \\ - \Pr\left[D(pp, \mathbf{g}, \mathbf{g}^a, \widehat{\mathbf{g}}, \widehat{\mathbf{g}}^a, \widehat{g}_0^b, \widehat{h}, \widehat{h}^b, \widehat{h}^c, e(\widehat{g}_0, \widehat{h})^{z}) = 1\right]|\end{aligned}$$

is negligible in k, for $(pp, sp) \leftarrow \mathsf{SampP}(k,n)$, for $\mathbf{g} \leftarrow \mathsf{SampG}(pp)$, for $\widehat{\mathbf{g}} = (\widehat{g}_0, \ldots, \widehat{g}_n) \leftarrow \widehat{\mathsf{SampG}}(pp, sp)$, for $\widehat{h}$ specified in sp, for e specified in pp, and for (uniform) $a, b, c, z \leftarrow \mathbb{Z}_N^*$.

Rerandomization. Fix $N \in \mathbb{N}$, $\mathbf{g}, \widehat{\mathbf{g}}, \mathbf{g}^a, \widehat{\mathbf{g}}^a \in G^{n+1}$, $\widehat{g}_0^b \in G$, $\widehat{h}, \widehat{h}^b, \widehat{h}^c \in H$, and $\mathbf{T} = e(\widehat{g}_0, \widehat{h})^z \in G_T$, for $a, b, c, z \in \mathbb{Z}_N^*$.

Rerand_a-algorithm. $\mathsf{Rerand}_a(N, \mathbf{g}, \mathbf{g}^a, \widehat{\mathbf{g}}, \widehat{\mathbf{g}}^a, \widehat{g}_0^b, \widehat{h}, \widehat{h}^b, \widehat{h}^c, \mathbf{T})$ samples $r_1, t_1 \leftarrow \mathbb{Z}_N^*$ and outputs

$$(\mathbf{g}^{\bar{a}}, \widehat{\mathbf{g}}^{\bar{a}}, \widehat{g}_0^b, \widehat{h}^b, \widehat{h}^c, \mathbf{T_a}),$$

where

$$\mathbf{g}^{\bar{a}} = (g_0^{\bar{a}}, \ldots, g_n^{\bar{a}}), \text{ for}$$
$$g_0^{\bar{a}} = (g_0^a)^{r_1} \cdot g_0^{t_1} = g_0^{a \cdot r_1 + t_1} \text{ and } g_i^{\bar{a}} = (g_i^a)^{r_1} \cdot g_i^{t_1} = g_i^{a \cdot r_1 + t_1}, \text{ for all } i \in [n],$$
$$\widehat{\mathbf{g}}^{\bar{a}} = (\widehat{g}_0^{\bar{a}}, \ldots, \widehat{g}_n^{\bar{a}}), \text{ for}$$
$$\widehat{g}_0^{\bar{a}} = (\widehat{g}_0^a)^{r_1} \cdot \widehat{g}_0^{t_1} = \widehat{g}_0^{a \cdot r_1 + t_1} \text{ and } \widehat{g}_i^{\bar{a}} = (\widehat{g}_i^a)^{r_1} \cdot \widehat{g}_i^{t_1} = g_i^{a \cdot r_1 + t_1}, \text{ for all } i \in [n],$$
$$\mathbf{T_a} = \mathbf{T}^{r_1} \cdot e(\widehat{g}_0^b, \widehat{h}^c)^{t_1} = \mathbf{T}^{r_1} \cdot e(\widehat{g}_0, \widehat{h})^{b \cdot c \cdot t_1}$$

If $z = abc$, then $\bar{a}$ is uniformly distributed in $\mathbb{Z}_N$ and $\mathbf{T_a} = \mathbf{T}^{\bar{a}bc}$. If $z \neq abc$, then $\bar{a}$ is uniformly distributed in $\mathbb{Z}_N$ and $\mathbf{T_a} = e(\widehat{g}_0, \widehat{h})^{zr_1 + bct_1}$, where $zr_1 + bct_1$ is uniformly distributed in $\mathbb{Z}_N$.

Rerand_b-algorithm. $\mathsf{Rerand}_b(N, \mathbf{g}, \mathbf{g}^a, \widehat{\mathbf{g}}, \widehat{\mathbf{g}}^a, \widehat{g}_0^b, \widehat{h}, \widehat{h}^b, \widehat{h}^c, \mathbf{T})$ samples $r_2, t_2 \leftarrow \mathbb{Z}_N^*$ and outputs

$$(\mathbf{g}^a, \widehat{\mathbf{g}}^a, \widehat{g}_0^{\bar{b}}, \widehat{h}^{\bar{b}}, \widehat{h}^c, \mathbf{T_b}),$$

where

$$\widehat{g}_0^{\bar{b}} = (\widehat{g}_0^b)^{r_2} \cdot \widehat{g}_0^{t_2} = \widehat{g}_0^{b \cdot r_2 + t_2},$$
$$\widehat{h}^{\bar{b}} = (\widehat{h}^b)^{r_2} \cdot \widehat{h}^{t_2} = \widehat{h}^{b \cdot r_2 + t_2},$$
$$\mathbf{T_b} = \mathbf{T}^{r_2} \cdot e(\widehat{g}_0^a, \widehat{h}^c)^{t_2} = \mathbf{T}^{r_2} \cdot e(\widehat{g}_0, \widehat{h})^{a \cdot c \cdot t_2}.$$

If $z = abc$, then $\bar{b}$ is uniformly distributed in $\mathbb{Z}_N$ and $\mathbf{T_b} = \mathbf{T}^{a\bar{b}c}$. If $z \neq abc$, then $\bar{b}$ is uniformly distributed in $\mathbb{Z}_N$ and $\mathbf{T_b} = e(\widehat{g}_0, \widehat{h})^{zr_2 + act_2}$, where $zr_2 + act_2$ is uniformly distributed in $\mathbb{Z}_N$.

Rerand_c**-algorithm.** $\mathsf{Rerand}_c(N, \mathbf{g}, \mathbf{g}^a, \widehat{\mathbf{g}}, \widehat{\mathbf{g}}^a, \widehat{g}_0^b, \widehat{h}, \widehat{h}^b, \widehat{h}^c, \mathbf{T})$ samples $r_3, t_3 \leftarrow \mathbb{Z}_N^*$ and outputs

$$(\mathbf{g}^a, \widehat{\mathbf{g}}^a, \widehat{g}_0^b, \widehat{h}^b, \widehat{h}^{\bar{c}}, \mathbf{T_c}),$$

where

$$\widehat{h}_0^{\bar{c}} = (\widehat{h}_0^c)^{r_3} \cdot \widehat{h}_0^{t_3} = \widehat{h}_0^{c \cdot r_3 + t_3},$$
$$\mathbf{T_c} = \mathbf{T}^{r_3} \cdot e(\widehat{g}_0^a, \widehat{h}^b)^{t_3} = \mathbf{T}^{r_3} \cdot e(\widehat{g}_0, \widehat{h})^{a \cdot b \cdot t_3}.$$

If $z = abc$, then $\bar{c}$ is uniformly distributed in $\mathbb{Z}_N$ and $\mathbf{T_c} = \mathbf{T}^{ab\bar{c}}$. If $z \neq abc$, then $\bar{c}$ is uniformly distributed in $\mathbb{Z}_N$ and $\mathbf{T_c} = e(\widehat{g}_0, \widehat{h})^{zr_3 + abt_3}$, where $zr_3 + abt_3$ is uniformly distributed in $\mathbb{Z}_N$.

Rerand_{abc}**-algorithm.** $\mathsf{Rerand}_{abc}(N, \mathbf{g}, \mathbf{g}^a, \widehat{\mathbf{g}}, \widehat{\mathbf{g}}^a, \widehat{g}_0^b, \widehat{h}, \widehat{h}^b, \widehat{h}^c, \mathbf{T})$ outputs

$$(\mathbf{g}^{\bar{a}}, \widehat{\mathbf{g}}^{\bar{a}}, \widehat{g}_0^{\bar{b}}, \widehat{h}^{\bar{b}}, \widehat{h}^{\bar{c}}, \mathbf{T_{abc}})$$

by running $\mathsf{Rerand}_a(N, \mathbf{g}, \mathbf{g}^a, \widehat{\mathbf{g}}, \widehat{\mathbf{g}}^a, \widehat{g}_0^b, \widehat{h}, \widehat{h}^b, \widehat{h}^c, \mathbf{T}) \to (\mathbf{g}^{\bar{a}}, \widehat{\mathbf{g}}^{\bar{a}}, \widehat{g}_0^b, \widehat{h}^b, \widehat{h}^c, \mathbf{T_a})$ and take this output as new input $(N, \mathbf{g}, \mathbf{g}^{\bar{a}}, \widehat{\mathbf{g}}, \widehat{\mathbf{g}}^{\bar{a}}, \widehat{g}_0^b, \widehat{h}, \widehat{h}^b, \widehat{h}^c, \mathbf{T_a})$ for Rerand_b. Then take this output $(\mathbf{g}^{\bar{a}}, \widehat{\mathbf{g}}^{\bar{a}}, \widehat{g}_0^{\bar{b}}, \widehat{h}^{\bar{b}}, \widehat{h}^c, \mathbf{T_{ab}})$ as appropriate input for Rerand_c to get $(\mathbf{g}^{\bar{a}}, \widehat{\mathbf{g}}^{\bar{a}}, \widehat{g}_0^{\bar{b}}, \widehat{h}^{\bar{b}}, \widehat{h}^{\bar{c}}, \mathbf{T_{abc}})$.

The input exponents a, b, c and z for all algorithms are required to be uniformly distributed in $\mathbb{Z}_N^*$, but if we reuse the outputs of $\mathsf{Rerand_a}$ and $\mathsf{Rerand_b}$, then $\bar{a}$ and $\bar{b}$ are uniformly distributed in $\mathbb{Z}_N$. However, the uniform distribution in $\mathbb{Z}_N$ is statistically indistinguishable from the uniform distribution in $\mathbb{Z}_N^*$, since for $a \leftarrow \mathbb{Z}_N^*, \bar{a} \leftarrow \mathbb{Z}_N$ the statistical distance $\mathsf{SD}(a\,;\,\bar{a}) = \frac{1}{2}\sum_{x \in \mathbb{Z}_N} |\Pr[a = x] - \Pr[\bar{a} = x]| = \frac{N - \varphi(N)}{N}$ is negligible in k, because for $N = p_1 \cdot \ldots \cdot p_{n'}$, where $n' \in \mathbf{O}(1)$ and p_s denotes the smallest k-bit prime factor of N, we have $\frac{N-\varphi(N)}{N} \overset{(*)}{\leq} \frac{N}{N} - \frac{N}{N} + \sum_{l=1}^{n'} \binom{n'}{l} \frac{1}{p_s^l} \leq c(n') \cdot \frac{1}{p_s} \in \mathbf{O}(2^{-k})$, for a constant $c(n')$ depending on n'. (Note that $(*)$ holds due to $\frac{\varphi(N)}{N} \geq \frac{N}{N} + \sum_{l=1}^{n'} \binom{n'}{l} \frac{1}{p_s^l}$.) So, if $z = abc$, then $\bar{a}, \bar{b}, \bar{c}$ are uniformly distributed in $\mathbb{Z}_N$ and $\mathbf{T_{abc}} = \mathbf{T}^{\bar{a}\bar{b}\bar{c}}$. If $z \neq abc$, then $\bar{a}, \bar{b}, \bar{c}$ are uniformly distributed in $\mathbb{Z}_N$ and, for $z_a := zr_1 + bct_1, z_{ab} := z_a r_2 + \bar{a}ct_2$ and $z_{abc} := z_{ab} r_3 + \bar{a}\bar{b}t_3$, we have $\mathbf{T_{abc}} = e(\widehat{g}_0, \widehat{h})^{z_{abc}}$, where z_a, z_{ab} and z_{abc} are all uniformly distributed in $\mathbb{Z}_N$.

Lemma 4.10 (Game 3 to Game 4, full security). *Let* G *be a group generator and* $\mathsf{Rerand_{abc}}$, $\mathsf{Rerand_a}$ *rerandomization algorithms, all as defined above. If* ENDSG *is an ENDSG system, s-BDDH holds, and* H *is a universal hash function, Game 3 and Game 4 are computationally indistinguishable. Concretely, for any PPT adversary A with at most $q' = q'(k)$ extraction queries per instance and running time t in the (μ, q)-IBE-IND-CPA security experiment with* IBE*, there is a distinguisher D with running time $t' \approx t + \mathbf{O}(\mu n k^c (q + q'))$, for some constant $c \in \mathbb{N}$, such that*

$$|\Pr[S_{A,3}] - \Pr[S_{A,4}]| \leq \mathsf{Adv}^{\text{s-bddh}}_{\mathsf{ENDSG},\mathsf{G},D}(k, 2n) + \mu q \cdot \mathbf{O}(2^{-k}). \tag{10}$$

Proof. In Game 3, each challenge ciphertext carries a b-dependent A-chosen message, for $b \leftarrow \{0,1\}$, while in Game 4, each challenge ciphertext message is replace by uniform k-length b-independent bitstring.

Description. D is provided with challenge input $(pp, \mathbf{g}, \mathbf{g}^a, \widehat{\mathbf{g}}, \widehat{\mathbf{g}}^a, \widehat{g}_0^b, \widehat{h}, \widehat{h}^b, \widehat{h}^c, \mathbf{T})$, where $\mathbf{T}$ is either $e(\widehat{g}_0, \widehat{h})^{abc}$ or $e(\widehat{g}_0, \widehat{h})^z$, for $(pp, sp) \leftarrow \mathsf{SampP}(k, 2n)$, for $\mathbf{g} \leftarrow \mathsf{SampG}(pp)$, for $\widehat{\mathbf{g}} = (\widehat{g}_0, \ldots, \widehat{g}_n) \leftarrow \widehat{\mathsf{SampG}}(pp, sp)$, for $\widehat{h}$ specified in sp, for e specified in pp, and for $a, b, c, z \leftarrow \mathbb{Z}_N^*$. First, D samples $(msk_j)_j \leftarrow (H)^\mu$, sets $mpk_j := (pp, \mathsf{H}, m(msk_j))$, for all j, for $\mathsf{H} \leftarrow \mathcal{UH}$, for m specified in pp, and sends $(mpk_j)_j$ to A. Further, D defines a truly random function $\widehat{\mathsf{R}} : [\mu] \times \{0,1\}^n \to \langle \widehat{h} \rangle$. During the experiment, D answers instance-j extraction queries for $id \in \mathcal{ID}$ as

$$\overline{\mathsf{Ext}}(pp, msk_j \cdot \widehat{\mathsf{R}}(j, id), id; \mathsf{SampH}(pp)),$$

for all j. Further, A may adaptively query its Enc'-oracle; for A-chosen instance-j challenge identity $id^*_{j,i'} = id^*_{j,i',1} \ldots, id^*_{j,i',n} \in \mathcal{ID}$ and equal-length messages $(M^*_{j,i',0}, M^*_{j,i',1}) \in (\mathcal{M})^2$, for all $(j, i') \in [\mu] \times [q]$. For each fresh instance-j challenge identity $id^*_{j,i'}$ (i.e., $id^*_{j,i'}$ was not queried before by A in instance j), D computes $(\mathbf{g}^{a_{j,i'}}, \widehat{\mathbf{g}}^{a_{j,i'}}, \widehat{g}_0^{b_{j,i'}}, \widehat{h}^{b_{j,i'}}, \widehat{h}^{c_{j,i'}}, \mathbf{T}_{j,i'}) \leftarrow \mathsf{Rerand}_{\mathsf{abc}}(N, \mathbf{g}, \mathbf{g}^a, \widehat{\mathbf{g}}, \widehat{\mathbf{g}}^a, \widehat{g}_0^b, \widehat{h}, \widehat{h}^b, \widehat{h}^c, \mathbf{T})$ and returns

$$((g_0\widehat{g}_0)^{a_{j,i'}}, (\prod_{i=1}^{n} g_{2i-id^*_{j,i',i}} \widehat{g}_{2i-id^*_{j,i',i}})^{a_{j,i'}}, \mathsf{H}(e((g_0\widehat{g}_0)^{a_{j,i'}}, msk_j) \cdot \mathbf{T}_{j,i'}) \oplus M^*_{j,i',b})$$

to A, for $b \leftarrow \{0,1\}$, for $s_{j,i'} \leftarrow \mathbb{Z}^*_N$, for all (j, i'). For a requeried challenge identity $id^*_{j,i''}$ in instance j (where $(j, i'') \in [\mu] \times [q]$ is the index of that previous query in instance j), D computes $(\mathbf{g}^{a'_{j,i''}}, \widehat{\mathbf{g}}^{a'_{j,i''}}, \widehat{g}_0^{b_{j,i''}}, \widehat{h}^{b_{j,i''}}, \widehat{h}^{c_{j,i''}}, \mathbf{T}'_{j,i''}) \leftarrow \mathsf{Rerand}_{\mathsf{a}}(N, \mathbf{g}, \mathbf{g}^{a_{j,i''}}, \widehat{\mathbf{g}}, \widehat{\mathbf{g}}^{a_{j,i''}}, \widehat{g}_0^{b_{j,i''}}, \widehat{h}, \widehat{h}^{b_{j,i''}}, \widehat{h}^{c_{j,i''}}, \mathbf{T}_{j,i''})$ and returns

$$((g_0\widehat{g}_0)^{a'_{j,i''}}, (\prod_{i=1}^{n} g_{2i-id^*_{j,i'',i}} \widehat{g}_{2i-id^*_{j,i'',i}})^{a'_{j,i''}}, \mathsf{H}(e((g_0\widehat{g}_0)^{a'_{j,i''}}, msk_j) \cdot \mathbf{T}'_{j,i''}) \oplus M^*_{j,i'',b})$$

to A, for all (j, i''). Eventually, A outputs a guess b'. D outputs 1 if $b' = b$ and A is valid in the sense of (μ, q)-IBE-IND-CPA, else outputs 0.

Analysis. The master public keys yield the correct distribution as well as the requested user secret keys. If $\mathbf{T} = e(\widehat{g}_0, \widehat{h})^{abc}$, then the challenge ciphertext exponents (as rerandomized in $\mathsf{Rerand}_{\mathsf{abc}}$ and $\mathsf{Rerand}_{\mathsf{a}}$, respectively) are distributed $\mathbf{O}(2^{-k})$-close to the challenge ciphertext exponents in Game 3. (See rerandomization paragraph above.) For a fresh challenge identity $id^*_{j,i'}$, we have that

$$\begin{aligned}
&((g_0\widehat{g}_0)^{a_{j,i'}}, (\prod_{i=1}^{n} g_{2i-id^*_{j,i',i}} \widehat{g}_{2i-id^*_{j,i',i}})^{a_{j,i'}}, \mathsf{H}(e((g_0\widehat{g}_0)^{a_{j,i'}}, msk_j) \cdot \mathbf{T}_{j,i'}) \oplus M^*_{j,i',b}) \\
&\overset{(*)}{=} ((g_0\widehat{g}_0)^{a_{j,i'}}, (\prod_{i=1}^{n} g_{2i-id^*_{j,i',i}} \widehat{g}_{2i-id^*_{j,i',i}})^{a_{j,i'}}, \mathsf{H}(e((g_0\widehat{g}_0)^{a_{j,i'}}, msk_j \cdot \widehat{h}^{b_{j,i'}c_{j,i'}})) \oplus M^*_{j,i',b}),
\end{aligned}$$

where $(*)$ holds due the orthogonality property of ENDSG. Note that we (implicitly) set $s_{j,i'} := a_{j,i'}$ and $\widehat{\gamma}_{j,i'} := b_{j,i'} \cdot c_{j,i'}$. For a requeried challenge identity $id^*_{j,i'}$, we rerandomize the previously used query value $a_{j,i'}$, for index (j, i'), and leave $\widehat{\gamma}_{j,i'}$ fixed. Otherwise, if $\mathbf{T} = e(\widehat{g}_0, \widehat{h})^z$, then the challenge ciphertext exponents are distributed $\mathbf{O}(2^{-k})$-close to the challenge ciphertext exponents in Game 4, i.e., we have that

$$\begin{aligned}
&((g_0\widehat{g}_0)^{a_{j,i'}}, (\prod_{i=1}^{n} g_{2i-id^*_{j,i',i}} \widehat{g}_{2i-id^*_{j,i',i}})^{a_{j,i'}}, \mathsf{H}(e((g_0\widehat{g}_0)^{a_{j,i'}}, msk_j) \cdot \mathbf{T}_{j,i'}) \oplus M^*_{j,i',b}) \\
&= ((g_0\widehat{g}_0)^{a_{j,i'}}, (\prod_{i=1}^{n} g_{2i-id^*_{j,i',i}} \widehat{g}_{2i-id^*_{j,i',i}})^{a_{j,i'}}, \mathsf{H}(e((g_0\widehat{g}_0)^{a_{j,i'}}, msk_j \cdot \widehat{h}^{z'_{j,i'}})) \oplus M^*_{j,i',b}),
\end{aligned}$$

for some uniform $a_{j,i'} \in \mathbb{Z}^*_N$ and $z'_{j,i'} := z_{j,i'} a^{-1}_{j,i'} \in \mathbb{Z}^*_N$ with overwhelming probability. Further, since H is a (randomly chosen) universal hash function, we have that $\mathsf{SD}((\mathsf{H}, \mathsf{H}(X)); (\mathsf{H}, U)) = \mathbf{O}(2^{-k})$, for $X \leftarrow G'_T$ and $U \leftarrow \{0,1\}^k$. Finally, via a union bound, (10) follows. □

Corollary 4.11 (Full (μ, q)-IBE-IND-CPA security of IBE)**.** *Let* G *be a group generator as defined above. If* ENDSG *is an ENDSG system, s-BDDH holds, and* H *is a universal hash function, then* IBE *is* (μ, q)*-IBE-IND-CPA-secure. Concretely, for any PPT adversary* A *with at most* $q' = q'(k)$ *extraction queries per instance and running time* t *in the* (μ, q)*-IBE-IND-CPA security experiment with* IBE*, there are distinguishers* D_1 *on LS1,* D_2 *on LS2,* D_3 *on NH,*

and D_4 on s-BDDH with running times $t'_1 \approx t'_2 \approx t'_3 \approx t'_4 \approx t + \mathbf{O}(\mu n k^c(q+q'))$, respectively, some constant $c \in \mathbb{N}$, with

$$\begin{aligned}\mathsf{Adv}^{(\mu,q)\text{-ibe-ind-cpa}}_{\mathsf{IBE},A}(k,n) \leq\ & \mathsf{Adv}^{\text{ls1}}_{\mathsf{ENDSG},\mathsf{G},D_1}(k,2n) + 2n \cdot \mathsf{Adv}^{\text{ls2}}_{\mathsf{ENDSG},\mathsf{G},D_2}(k,2n) \\ & + n \cdot \mathsf{Adv}^{\text{nh}}_{\mathsf{ENDSG},\mathsf{G},D_3}(k,2n,\mu q') + \mathsf{Adv}^{\text{s-bddh}}_{\mathsf{ENDSG},\mathsf{G},D_4}(k,2n) \\ & + \mu q \cdot \mathbf{O}(2^{-k}), \end{aligned} \tag{11}$$

for group generator G defined as above.

Proof. Taking (2), (3), (4), (5), (6), (7), (10), and (9) together, yields (11). □

5 Instantiations of ENDSGs in composite-order groups

Assumptions in groups with composite order. We slightly modify two (known) dual system assumptions (i.e., see DS1, DS3 below, and [11]) and define one (new) dual system assumption (see DS2 below). Further, we give a dual system variant of the Bilinear Decisional Diffie-Hellman assumption, dubbed DS-BDDH, and argue that DS-BDDH implies s-BDDH from Section 4. Let $\mathsf{G}(k,4)$ be a composite-order group generator that outputs group parameters $(G, H = G, G_T, N, e, g, g_{p_1}, g_{p_2}, g_{p_3}, g_{p_4})$ with the composite-order groups G, G_T, each of order $N = p_1 \cdots p_4$, for pairwise-distinct k-bit primes $(p_i)_i$. Further, g_{p_i} is a generator of the subgroup $G_{p_i} \subset G$ of order p_i, and g is a generator of G. More generally, we write $G_q \subseteq G$ for the unique subgroups of order q. The assumptions in groups with composite order are as follows:

Dual system assumption 1 (DS1). For any PPT adversary D, the function

$$\mathsf{Adv}^{\text{ds1}}_{\mathsf{G},D}(k) := |\Pr\left[D(pars, g'_{p_1}) = 1\right] - \Pr\left[D(pars, g'_{p_1p_2}) = 1\right]|$$

is negligible in k, for $(G, G_T, N, e, g, (g_{p_i})_i) \leftarrow \mathsf{G}(k,4)$,

$$pars := (G, G_T, N, e, g, g_{p_1}, g_{p_3}, g_{p_4}), \text{ and } g'_{p_1} \xleftarrow{g} G_{p_1},\ g'_{p_1p_2} \xleftarrow{g} G_{p_1p_2}.$$

Dual system assumption 2 (DS2). For any PPT adversary D, the function

$$\mathsf{Adv}^{\text{ds2}}_{\mathsf{G},D}(k) := |\Pr\left[D(pars, g'_{p_1p_2}) = 1\right] - \Pr\left[D(pars, g'_{p_1p_3}) = 1\right]|$$

is negligible in k, for $(G, G_T, N, e, g, (g_{p_i})_i) \leftarrow \mathsf{G}(k,4)$,

$$pars := (G, G_T, N, e, g, g_{p_1}, g_{p_4}, g_{p_1p_2}, g_{p_2p_3}),$$

$$g_{p_1p_2} \xleftarrow{g} G_{p_1p_2},\ g_{p_2p_3} \xleftarrow{g} G_{p_2p_3}, \text{ and } g'_{p_1p_2} \xleftarrow{g} G_{p_1p_2},\ g'_{p_1p_3} \xleftarrow{g} G_{p_1p_3}.$$

Dual system assumption 3 (DS3). For any PPT adversary D, the function

$$\mathsf{Adv}^{\text{ds3}}_{\mathsf{G},D}(k) := |\Pr\left[D(pars, g_{p_2}^{xy}, g_{p_3}^{xy}) = 1\right] - \Pr\left[D(pars, g_{p_2}^{xy+\gamma'}, g_{p_3}^{xy+\gamma'}) = 1\right]|$$

is negligible in k, for $(G, G_T, N, e, g, (g_{p_i})_i) \leftarrow \mathsf{G}(k,4)$,

$$pars := (G, G_T, N, e, g, (g_{p_i})_i, g_{p_2}^x \widehat{X}_4, g_{p_2}^y \widehat{Y}_4, g_{p_3}^x \widetilde{X}_4, g_{p_3}^y \widetilde{Y}_4),$$

$$\widehat{X}_4, \widetilde{X}_4, \widehat{Y}_4, \widetilde{Y}_4 \xleftarrow{g} G_{p_4},\ x, y, \leftarrow \mathbb{Z}_N^*, \text{ and } \gamma' \leftarrow \mathbb{Z}_N^*.$$

Dual system bilinear DDH assumption (DS-BDDH). For any PPT adversary D, the function

$$\mathsf{Adv}^{\text{ds-bddh}}_{\mathsf{G},D}(k) := |\Pr\left[D(pars, e(g_{p_2}, g_{p_2})^{abc}) = 1\right] - \Pr\left[D(pars, e(g_{p_2}, g_{p_2})^{z}) = 1\right]|$$

is negligible in k, for $(G, G_T, N, e, g, (g_{p_i})_i) \leftarrow \mathsf{G}(k, 4)$, for

$$pars := (G, G_T, N, e, g, (g_{p_i})_i, g^a_{p_1}, g^a_{p_2}, g^b_{p_2}, g_{p_2p_4}, g^b_{p_2p_4}, g^c_{p_2p_4}),$$

for $g_{p_2p_4} \xleftarrow{g} G_{p_2p_4}$, $a, b, c, z \leftarrow \mathbb{Z}^*_N$.

Lemma 5.1 (DS-BDDH implies s-BDDH). *For any PPT adversary D with running time t on s-BDDH there is a distinguisher D' on DS-BDDH with running time $t' \approx t$ such that*

$$\mathsf{Adv}^{\text{ds-bddh}}_{\mathsf{G},D'}(k) = \mathsf{Adv}^{\text{s-bddh}}_{\mathsf{G},D}(k, n), \tag{12}$$

for G as defined above. Hence, s-BDDH holds under DS-BDDH.

Proof. **Description.** The challenge input to D' is provided as $(pars, \mathbf{T})$, where $\mathbf{T}$ is either $e(g_{p_2}, g_{p_2})^{abc} \leftarrow G_{p_1}$ or $e(g_{p_2}, g_{p_2})^{z}$, for

$$pars = (G, G_T, N, e, g, (g_{p_i})_i, g^a_{p_1}, g^a_{p_2}, g^b_{p_2}, g_{p_2p_4}, g^b_{p_2p_4}, g^c_{p_2p_4}),$$

for $g_{p_2p_4} \xleftarrow{g} G_{p_2p_4}$, and for $a, b, c, z \leftarrow \mathbb{Z}^*_N$. First, D' sets the public parameter as $pp := (G, H := G, G_T, N, g, e, m, n, pars')$, for $m : h' \mapsto e(g_1, h')$, $pars' := (g_{p_1}, g_{p_4}, g^{\mathbf{w}}_{p_1}, h := g, h^{\mathbf{w}})$, for $\mathbf{w} \leftarrow (\mathbb{Z}^*_N)^n$, and for some integer n determined by D'. Then, D' sends

$$(pp, \mathbf{g} := (g^s_{p_1}, g^{s\cdot\mathbf{w}}_{p_1}), \mathbf{g}^a, \widehat{\mathbf{g}} := (g^{\hat{s}}_{p_2}, g^{\hat{s}\cdot\mathbf{w}}_{p_2}), \widehat{\mathbf{g}}^a, g^{b\cdot\hat{s}}_{p_2}, g_{p_2p_4}, g^b_{p_2p_4}, g^c_{p_2p_4}, \mathbf{T}),$$

for $s, \hat{s} \leftarrow \mathbb{Z}^*_N$, to D. Finally, D outputs a value which D' forwards to its own challenger.

Analysis. Note that pp is distributed as defined in s-BDDH. If $\mathbf{T} = e(g_{p_2}, g_{p_2})^{abc}$, then $\Pr\left[D'(pars, e(g_{p_2}, g_{p_2})^{abc}) = 1\right] = \Pr\left[D(pp, \mathbf{g}, \mathbf{g}^a, \widehat{\mathbf{g}}, \widehat{\mathbf{g}}^a, g^{b\hat{s}}_{p_2}, g_{p_2p_4}, g^b_{p_2p_4}, g^c_{p_2p_4}, e(g_{p_2}, g_{p_2})^{abc}) = 1\right]$ follows. Otherwise, if $\mathbf{T} = e(g_{p_2}, g_{p_2})^{z}$ holds, then we have that $\Pr\left[D'(pars, e(g_{p_2}, g_{p_2})^{z}) = 1\right] = \Pr\left[D(pp, \mathbf{g}, \mathbf{g}^a, \widehat{\mathbf{g}}, \widehat{\mathbf{g}}^a, g^{b\hat{s}}_{p_2}, g_{p_2p_4}, g^b_{p_2p_4}, g^c_{p_2p_4}, e(g_{p_2}, g_{p_2})^{z}) = 1\right]$. Hence, (12) follows. □

ENDSGs in groups with composite order. Let $\mathsf{G}(k, 4)$ be as defined above. For simplicity, we write $g_i := g_{p_i}$ and $g_{ij} := g_{p_ip_j}$, for all $(i, j) \in [4] \times [4]$. We instantiate ENDSGs $\mathsf{ENDSG}_{\mathsf{co}} = (\mathsf{SampP}, \mathsf{SampG}, \mathsf{SampH}, \widehat{\mathsf{SampG}}, \widetilde{\mathsf{SampG}})$ in composite-order groups as follows:

Parameter sampling. $\mathsf{SampP}(k, n)$, given k and n, samples $(G, H, G_T, (p_i)_i, e, g, h, (g_i)_i) \leftarrow \mathsf{G}(k, 4)$ and outputs $pp := (G, H, G_T, N, g, e, m, n, pars)$ and $sp := (\widehat{h}, \widetilde{h}, \widehat{pars}, \widetilde{pars})$, for

- $m : H \to G_T, h' \mapsto e(g_1, h')$,
- $pars := (g_1, g_4, g^{\mathbf{w}}_1, h, h^{\mathbf{w}} \cdot \mathbf{R_4})$, for $\mathbf{w} \leftarrow (\mathbb{Z}^*_N)^n$, $\mathbf{R}_4 \xleftarrow{g} (G_{p_4})^n$,
- $\widehat{h} \xleftarrow{g} G_{p_2p_4}, \widetilde{h} \xleftarrow{g} G_{p_3p_4}$,
- $\widehat{pars} := (g_2, g^{\mathbf{w}}_2)$, $\widetilde{pars} := (g_3, g^{\mathbf{w}}_3)$.

G-Group sampling. $\mathsf{SampG}(pp)$, on input pp, samples $s \leftarrow \mathbb{Z}^*_N$ and outputs $(g^s_1, g^{s\cdot\mathbf{w}}_1)$.

H-Group sampling. $\mathsf{SampH}(pp)$, on input pp, samples $r \leftarrow \mathbb{Z}^*_N$ and outputs $(h^r, h^{r\cdot\mathbf{w}} \cdot \mathbf{R}'_4)$, for $\mathbf{R}'_4 \xleftarrow{g} (G_{p_4})^n$.

Semi-functional G-group sampling 1. $\widehat{\mathsf{SampG}}(pp, sp)$, on input pp and sp, samples $s \leftarrow \mathbb{Z}^*_N$ and outputs $(g^s_2, g^{s\cdot\mathbf{w}}_2)$.

Semi-functional G-group sampling 2. $\widetilde{\mathsf{SampG}}(pp, sp)$, on input pp and sp, samples $s \leftarrow \mathbb{Z}_N^*$ and outputs $(g_3^s, g_3^{s \cdot \mathbf{w}})$.

Correctness of $\mathsf{ENDSG_{co}}$. For all $k, n \in \mathbb{N}$ and group parameters $(G, H, G_T, N, e, g, h, (g_i)_i) \leftarrow \mathsf{G}(k, 4)$, we have:

Associativity. For all $s, r \leftarrow \mathbb{Z}_N^*$, for all $(g_1^s, g_1^{s \cdot \mathbf{w}}) \leftarrow \mathsf{SampG}(pp; s)$, for all $(h^r, h^{r \cdot \mathbf{w}} \cdot \mathbf{R'}_4) \leftarrow \mathsf{SampH}(pp; r)$, for $\mathbf{R'}_4 = (R'_i)_i \in (G_{p_4})^n$, it holds that $e(g_1^s, h^{r \cdot w_i} \cdot R'_i) = e(g_1^s, h^{r \cdot w_i}) = e(g_1^{s \cdot w_i}, h^r)$for all $i \in [n]$, and for $\mathbf{w} = (w_1, \ldots, w_n) \in (\mathbb{Z}_N^*)^n$.

Projective. For all $s \leftarrow \mathbb{Z}_N^*$, for all $h' \in H$, it holds that $m(h')^s = e(g_1, h')^s = e(g_1^s, h')$. (Note that g_1^s is the first output of $\mathsf{SampG}(pp; s)$.)

Security of $\mathsf{ENDSG_{co}}$. Let G be a composite-order group generator as defined above, for all $k, n, \in \mathbb{N}$, for all $(pp, sp) \leftarrow \mathsf{SampP}(k, n)$, we have:

Orthogonality. For $\widehat{h}, \widetilde{h}$ specified in sp, we have $m(\widehat{h}) = e(g_1, \widehat{h}) = e((g^{p_2 p_3 p_4})^{\gamma_{g_1}}, (g^{p_1 p_3})^{\gamma_{\widehat{h}}}) = 1$, $m(\widetilde{h}) = e(g_1, \widetilde{h}) = e((g^{p_2 p_3 p_4})^{\gamma_{g_1}}, (g^{p_1 p_2})^{\gamma_{\widetilde{h}}}) = 1$for suitable exponents $\gamma_{g_1}, \gamma_{\widehat{h}}, \gamma_{\widetilde{h}} \in \mathbb{Z}_N^*$. Further, for g_1^s, $g_2^{s'}$, and $g_3^{s''}$ that are the first outputs of $\mathsf{SampG}(pp; s)$, $\widehat{\mathsf{SampG}}(pp, sp; s')$, and $\widetilde{\mathsf{SampG}}(pp, sp; s'')$, for $s, s', s'' \leftarrow \mathbb{Z}_N^*$, we have $e(g_1^s, \widehat{h}) = e(g_1^s, \widetilde{h}) = e(g_2^{s'}, \widetilde{h}) = e(g_3^{s''}, \widehat{h}) = 1$.

G- and H-subgroups. Since g_1, g_2, and g_3 are generators of subgroups G_{p_1}, G_{p_2}, and G_{p_3} of coprime order, the outputs of SampG, $\widehat{\mathsf{SampG}}$, and $\widetilde{\mathsf{SampG}}$ are uniform over the generators, which generates nontrivial subgroups of G of coprime order. Since h is a generator of H and $\mathbf{R'}_4$ is uniform over the generators of $(G_{p_4})^n$, the output of SampH is uniformly distributed over the generators of H.

Non-degeneracy. For the first output g_2^s of $\widehat{\mathsf{SampG}}(pp, sp; s)$ (with uniform $s \in \mathbb{Z}_N^*$), and for $\widehat{h} \in G_{p_2 p_3}$ as specified in sp, it holds that $e(g_2^s, \widehat{h}) = e(g_2, \widehat{h})^s$ is uniformly distributed over the generators of the subgroup generated by $e(g_2, \widehat{h})$. Similarly, for the first output g_3^s of $\widetilde{\mathsf{SampG}}(pp, sp; s)$, it holds that $e(g_3^s, \widetilde{h}) = e(g_3, \widetilde{h})^s$ is distributed uniformly over the generators of the subgroup generated by $e(g_3, \widetilde{h})$.

Left-subgroup indistinguishability 1. We prove the following lemma

Lemma 5.2 (DS1 implies LS1). *For any PPT adversary D with running time t on LS1 of $\mathsf{ENDSG_{co}}$ as defined above there is a distinguisher D' on DS1 with running time $t' \approx t$ such that*

$$\mathsf{Adv}^{\mathrm{ds1}}_{\mathsf{G},D'}(k) = \mathsf{Adv}^{\mathrm{ls1}}_{\mathsf{ENDSG_{co}},\mathsf{G},D}(k, n), \tag{13}$$

for G as defined above. Hence, LS1 holds under DS1.

Proof. **Description.** The challenge input to D' is provided as $(pars, \mathbf{T})$, where $\mathbf{T}$ is either $g'_1 \leftarrow G_{p_1}$ or $g'_{12} \leftarrow G_{p_1 p_2}$, for $pars = (G, G_T, N, e, g, g_1, g_3, g_4)$. First, D' sets the public parameter as $pp := (G, H := G, G_T, N, g, e, m, n, pars')$, for $m : h' \mapsto e(g_1, h')$, $pars' := (g_1, g_4, g_1^{\mathbf{w}}, h := g, h^{\mathbf{w}})$, for $\mathbf{w} \leftarrow (\mathbb{Z}_N^*)^n$, and for some integer n determined by D'. Then, D' sends $(pp, \mathbf{T}, \mathbf{T}^{\mathbf{w}})$ to D. Finally, D outputs a value which D' forwards to its own challenger.

Analysis. Note that pp is distributed as defined in LS1. If $\mathbf{T} = g'_1$, then $(g'_1, (g'_1)^{\mathbf{w}})$ is distributed as the output of $\mathsf{SampG}(pp)$ as needed and, hence, $\Pr[D'(pars, g'_1) = 1] = \Pr[D(pp, (g'_1, (g'_1)^{\mathbf{w}})) = 1]$ follows. Otherwise, if $\mathbf{T} = g'_{12}$, then $(g'_{12}, (g'_{12})^{\mathbf{w}})$ is distributed as $\mathsf{SampG}(pp) \cdot \widehat{\mathsf{SampG}}(pp, sp)$, for suitable sp, as desired and, hence, we have that $\Pr[D'(pars, g'_{12}) = 1] = \Pr[D(pp, (g'_{12}, (g'_{12})^{\mathbf{w}})) = 1]$. As a consequence, (13) follows. □

Left-subgroup indistinguishability 2. We prove the following lemma

Lemma 5.3 (DS2 implies LS2). *For any PPT adversary D with running time t on LS2 of $\mathsf{ENDSG_{co}}$ defined as above there is a distinguisher D' on DS2 with running time $t' \approx t$ such that*

$$\mathsf{Adv}^{\mathrm{ls2}}_{\mathsf{ENDSG_{co}},\mathsf{G},D}(k,n) = \mathsf{Adv}^{\mathrm{ds2}}_{\mathsf{G},D'}(k), \tag{14}$$

for G as defined above. Hence, LS2 holds under DS2.

Proof. **Description.** The challenge input to D' is provided as $(pars, \mathbf{T})$, where $\mathbf{T}$ is either $g'_{12} \leftarrow G_{p_1p_2}$ or $g'_{13} \leftarrow G_{p_1p_3}$, for $pars = (G, G_T, N, e, g, g_1, g_4, g_{12}, g_{23})$. First, D' defines the public parameter as $pp := (G, H := G, G_T, N, g, e, m, n, pars')$, for $m : h' \mapsto e(g_1, h')$, $pars' := (g_1, g_4, g_1^{\mathbf{w}}, h := g, h^{\mathbf{w}})$, for $\mathbf{w} \leftarrow (\mathbb{Z}_N^*)^n$, and for some integer n determined by D'. Then, D' sends $(pp, g_{23}g_4^{\gamma}, g_{12}, \mathbf{T}, \mathbf{T}^{\mathbf{w}})$, for $\gamma \leftarrow \mathbb{Z}_N^*$, to D. Eventually, D outputs a value which is forwarded by D' to its own challenger.

Analysis. Note that pp is distributed as defined in LS2. If $\mathbf{T} = g'_{12}$, then $(g'_{12}, (g'_{12})^{\mathbf{w}})$ is distributed as $\mathsf{SampG}(pp) \cdot \widehat{\mathsf{SampG}}(pp, sp)$, for suitable sp, as needed and, hence, we have that $\Pr[D'(pars, g'_{12}) = 1] = \Pr[D(pp, g_{23}g_4^{\gamma}, g_{12}, (g'_{12}, (g'_{12})^{\mathbf{w}})) = 1]$ follows. Otherwise, if $\mathbf{T} = g'_{13}$, then $(g'_{13}, (g'_{13})^{\mathbf{w}})$ is distributed as $\mathsf{SampG}(pp) \cdot \widetilde{\mathsf{SampG}}(pp, sp)$, for suitable sp, as desired and, hence, $\Pr[D'(pars, g'_{13}) = 1] = \Pr[D(pp, g_{23}g_4^{\gamma}, g_{12}, (g'_{13}, (g'_{13})^{\mathbf{w}})) = 1]$ holds. As a consequence, (14) follows. □

Nested-hiding indistinguishability. We prove the following lemma

Lemma 5.4 (DS3 implies NH). *For any PPT adversary D with running time t on NH of $\mathsf{ENDSG_{co}}$ there is a distinguisher D' on DS3 with running time $t' \approx t$ such that*

$$\mathsf{Adv}^{\mathrm{nh}}_{\mathsf{ENDSG_{co}},\mathsf{G},D}(k,n,q') \leq \mathsf{Adv}^{\mathrm{ds3}}_{\mathsf{G},D'}(k), \tag{15}$$

for $q' \in \mathbb{N}$ and G as defined above. Hence, NH holds under DS3.

Proof. The proof follows the same strategy as shown in Chen and Wee's work [11] except that we have to integrate two coprime-order semi-functional generators $\widehat{h}$ and $\widetilde{h}$ instead of just one as in [11].

Description. The challenge input to D' is provided as $(pars, \mathbf{T})$, where $\mathbf{T} := (\widehat{\mathbf{T}}, \widetilde{\mathbf{T}})$ is either (g_2^{xy}, g_3^{xy}) or $(g_2^{xy+\gamma'}, g_3^{xy+\gamma'})$, for

$$pars =: (G, G_T, N, e, g_1, g_2, g_3, g_4, g_2^x\widehat{X}_4, g_2^y\widehat{Y}_4, g_3^x\widetilde{X}_4, g_3^y\widetilde{Y}_4),$$

for $\widehat{X}_4, \widehat{Y}_4, \widetilde{X}_4, \widetilde{Y}_4 \xleftarrow{g} G_{p_4}$, $x, y \leftarrow \mathbb{Z}_N^*$, and for $\gamma' \leftarrow \mathbb{Z}_N^*$. Furthermore, D' receives an auxiliary input $i \in [\lfloor \frac{n}{2} \rfloor]$, for some integer $n \in \mathbb{N}$ determined by D'. First, D' samples $r, \hat{r}, \tilde{r}, \hat{s}, \tilde{s} \leftarrow \mathbb{Z}_N^*$, $\mathbf{R'}_4 \xleftarrow{g} (G_{p_4})^n$, $\mathbf{w'} \leftarrow (\mathbb{Z}_N^*)^n$, and sets

$$h := (g_1g_2g_3g_4)^r, \qquad \widehat{h} := (g_2g_4)^{\hat{r}}, \qquad \widetilde{h} := (g_3g_4)^{\tilde{r}},$$
$$\widehat{\mathbf{g}}_{-(2i-1)} := (g_2^{\hat{s}}, g_2^{\hat{s}\mathbf{w'}})_{-(2i-1)}, \qquad \widetilde{\mathbf{g}}_{-2i} := (g_3^{\tilde{s}}, g_3^{\tilde{s}\mathbf{w'}})_{-(2i)},$$

where h, $\widehat{h}$, and $\widetilde{h}$ are generators of G, $G_{p_2p_4}$, and $G_{p_3p_4}$. Then, D' defines public parameter as

$$pp := (G, H := G, G_T, N, g, e, n, m, pars'),$$

for $m : h' \mapsto e(g_1, h')$ and

$$pars' := (g_1, g_4, g_1^{\mathbf{w}'}, h, h^{\mathbf{w}'}(g_2^y \widehat{Y}_4)^{r\mathbf{e}_{2i-1}}(g_3^y \widetilde{Y}_4)^{r\mathbf{e}_{2i}}\mathbf{R}'_4) = (g_1, g_4, g_1^{\mathbf{w}}, h, h^{\mathbf{w}}\mathbf{R}_4),$$

where $\mathbf{e}_j$ is the j-th unit vector of length n and, implicitly, we have

$$\mathbf{w} = \begin{cases} \mathbf{w}' \mod p_1p_4 \\ \mathbf{w}' + y \cdot \mathbf{e}_{2i-1} \mod p_2 \\ \mathbf{w}' + y \cdot \mathbf{e}_{2i} \mod p_3 \end{cases} \quad \text{and} \quad \mathbf{R}_4 = \mathbf{R}'_4 + \widehat{Y}_4^r \cdot \mathbf{e}_{2i-1} + \widetilde{Y}_4^r \cdot \mathbf{e}_{2i}.$$

Now, by running the algorithm from [12, Lemma 6] on input $(1^{q'}, (g_2, g_4, g_2^x \widehat{X}_4, g_2^y \widehat{Y}_4, \widehat{\mathbf{T}}))$ and on input $(1^{q'}, (g_3, g_4, g_3^x \widetilde{X}_4, g_3^y \widetilde{Y}_4, \widetilde{\mathbf{T}}))$, D' generates tuples

$$(g_2^{\hat{r}_j} \widehat{X}_{4,j}, \widehat{\mathbf{T}}_j)_{j=1}^{q'} \text{ and } (g_3^{\tilde{r}_j} \widetilde{X}_{4,j}, \widetilde{\mathbf{T}}_j)_{j=1}^{q'},$$

respectively, where

$$\widehat{\mathbf{T}}_j = \begin{cases} g_2^{\hat{r}_j y} \cdot \widehat{Y}_{4,j}, & \text{if } \widehat{\mathbf{T}} = g_2^{xy} \\ g_2^{\hat{r}_j y} \cdot \widehat{Y}_{4,j} \cdot g_2^{\hat{\gamma'}_j}, & \text{if } \widehat{\mathbf{T}} = g_2^{xy+\gamma'} \end{cases}, \qquad \widetilde{\mathbf{T}}_j = \begin{cases} g_3^{\tilde{r}_j y} \cdot \widetilde{Y}_{4,j}, & \text{if } \widetilde{\mathbf{T}} = g_3^{xy} \\ g_3^{\tilde{r}_j y} \cdot \widetilde{Y}_{4,j} \cdot g_3^{\tilde{\gamma'}_j}, & \text{if } \widetilde{\mathbf{T}} = g_3^{xy+\gamma'}. \end{cases}$$

Further, D' samples $r'_j \leftarrow \mathbb{Z}_N^*$, $\mathbf{X'}_{4,j} \xleftarrow{g} (G_{p_4})^n$, for all $j \in [q']$, and sends

$$(pp, \widehat{h}, \widetilde{h}, \widehat{\mathbf{g}}_{2i-1}, \widetilde{\mathbf{g}}_{2i}, (\mathbf{T}_1, \ldots, \mathbf{T}_{q'}))$$

to D, where

$$\begin{aligned} \mathbf{T}_j &= (h^{r'_j} \cdot g_2^{\hat{r}_j} \widehat{X}_{4,j} \cdot g_3^{\tilde{r}_j} \widetilde{X}_{4,j}, (h^{r'_j} \cdot g_2^{\hat{r}_j} \widehat{X}_{4,j} \cdot g_3^{\tilde{r}_j} \widetilde{X}_{4,j})^{\mathbf{w}'} \cdot \\ &\quad ((g_2^y \widehat{Y}_4)^{r'_j r} \widehat{\mathbf{T}}_j)^{\mathbf{e}_{2i-1}} \cdot ((g_3^y \widetilde{Y}_4)^{r'_j r} \widetilde{\mathbf{T}}_j)^{\mathbf{e}_{2i}} \mathbf{X'}_{4,j}) \\ &= \begin{cases} (h^{r_j}, h^{r_j \cdot \mathbf{w}} \cdot \mathbf{X}_{4,j}) & \text{if } \widehat{\mathbf{T}}_j = g_2^{\hat{r}_j y} \cdot \widehat{Y}_{4,j},\ \widetilde{\mathbf{T}}_j = g_3^{\tilde{r}_j y} \cdot \widetilde{Y}_{4,j} \\ (h^{r_j}, h^{r_j \cdot \mathbf{w}} \cdot g_2^{\hat{\gamma}_j \mathbf{e}_{2i-1}} \cdot g_3^{\tilde{\gamma}_j \mathbf{e}_{2i}} \cdot \mathbf{X}_{4,j}) & \text{if } \widehat{\mathbf{T}}_j = g_2^{\hat{r}_j y} \cdot \widehat{Y}_{4,j} \cdot g_2^{\hat{\gamma}_j},\ \widetilde{\mathbf{T}}_j = g_3^{\tilde{r}_j y} \cdot \widetilde{Y}_{4,j} \cdot g_3^{\tilde{\gamma}_j} \end{cases} \end{aligned}$$

for $h^{r_j} := h^{r'_j} \cdot g_2^{\hat{r}_j} \widehat{X}_{4,j} \cdot g_3^{\tilde{r}_j} \widetilde{X}_{4,j}$ and $\mathbf{X}_{4,j} := \mathbf{X'}_{4,j} + \widehat{Y}_4^{r'_j r} \mathbf{e}_{2i-1} + \widetilde{Y}_4^{r'_j r} \mathbf{e}_{2i}$ implicitly and $\mathbf{w}$ as above.

Analysis. Note that pp is distributed as defined in NH. If $\mathbf{T} = (g_2^{xy}, g_3^{xy})$, then $\widehat{\mathbf{T}}_j = g_2^{\hat{r}_j y} \cdot \widehat{Y}_{4,j}$ and $\widetilde{\mathbf{T}}_j = g_3^{\tilde{r}_j y} \cdot \widetilde{Y}_{4,j}$, for all $j \in [q']$, and, thus, $(\mathbf{T}_1, \ldots, \mathbf{T}_{q'})$ is distributed as $(\mathbf{h}_1, \ldots, \mathbf{h}_{q'})$, for suitable sp, as needed. Otherwise, if $\mathbf{T} = (g_2^{xy+\gamma'}, g_3^{xy+\gamma'})$, then $\widehat{\mathbf{T}}_j = g_2^{\hat{r}_j y} \cdot \widehat{Y}_{4,j} \cdot g_2^{\hat{\gamma}_j}$ and $\widetilde{\mathbf{T}}_j = g_3^{\tilde{r}_j y} \cdot \widetilde{Y}_{4,j} \cdot g_3^{\tilde{\gamma}_j}$ for all $j \in [q']$, and, thus, $(\mathbf{T}_1, \ldots, \mathbf{T}_{q'})$ is distributed as $(\mathbf{h'}_1, \ldots, \mathbf{h'}_{q'})$, for suitable sp, since $(\widehat{h}, g_2^{\hat{\gamma}_j} \cdot \widehat{Y}_{4,j})$ and $(\widetilde{h}, g_3^{\tilde{\gamma}_j} \cdot \widetilde{Y}_{4,j})$ are identically distributed as $(\widehat{h}, (\widehat{h})^{\hat{\gamma}_j} \cdot \widehat{Y}_{4,j})$ and $(\widetilde{h}, (\widetilde{h})^{\tilde{\gamma}_j} \cdot \widetilde{Y}_{4,j})$, respectively, for $\hat{\gamma}_j, \tilde{\gamma}_j \leftarrow \mathbb{Z}_N^*, \widehat{Y}_{4,j}, \widetilde{Y}_{4,j} \xleftarrow{g} G_{p_4}$, for all $j \in [q']$. □

Acknowledgements. We thank the anonymous reviewers for helpful remarks.

References

[1] Masayuki Abe, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, and Miyako Ohkubo. Tagged one-time signatures: Tight security and optimal tag size. In Kaoru Kurosawa and Goichiro Hanaoka, editors, *PKC 2013*, volume 7778 of *LNCS*, pages 312–331. Springer, February / March 2013. doi: 10.1007/978-3-642-36362-7_20.

[2] Mihir Bellare, Anand Desai, Eric Jokipii, and Phillip Rogaway. A concrete security treatment of symmetric encryption. In *38th FOCS*, pages 394–403. IEEE Computer Society Press, October 1997.

[3] Mihir Bellare, Anand Desai, David Pointcheval, and Phillip Rogaway. Relations among notions of security for public-key encryption schemes. In Hugo Krawczyk, editor, *CRYPTO'98*, volume 1462 of *LNCS*, pages 26–45. Springer, August 1998.

[4] Mihir Bellare, Alexandra Boldyreva, and Silvio Micali. Public-key encryption in a multi-user setting: Security proofs and improvements. In Bart Preneel, editor, *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 259–274. Springer, May 2000.

[5] Mihir Bellare, Brent Waters, and Scott Yilek. Identity-based encryption secure against selective opening attack. In Yuval Ishai, editor, *TCC 2011*, volume 6597 of *LNCS*, pages 235–252. Springer, March 2011.

[6] Olivier Blazy, Eike Kiltz, and Jiaxin Pan. (hierarchical) identity-based encryption from affine message authentication. In *Proceedings of CRYPTO (1) 2014*, number 8616 in Lecture Notes in Computer Science, pages 408–425. Springer, 2014.

[7] Alexandra Boldyreva. Strengthening security of RSA-OAEP. In Marc Fischlin, editor, *CT-RSA 2009*, volume 5473 of *LNCS*, pages 399–413. Springer, April 2009.

[8] Dan Boneh and Xavier Boyen. Short signatures without random oracles. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 56–73. Springer, May 2004.

[9] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 213–229. Springer, August 2001.

[10] David Cash, Eike Kiltz, and Victor Shoup. The twin Diffie-Hellman problem and applications. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 127–145. Springer, April 2008.

[11] Jie Chen and Hoeteck Wee. Fully, (almost) tightly secure IBE and dual system groups. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 435–460. Springer, August 2013. doi: 10.1007/978-3-642-40084-1_25.

[12] Jie Chen and Hoeteck Wee. Dual system groups and its applications — compact hibe and more. Cryptology ePrint Archive, Report 2014/265, 2014. `http://eprint.iacr.org/`.

[13] David Mandell Freeman. Converting pairing-based cryptosystems from composite-order groups to prime-order groups. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 44–61. Springer, May 2010.

[14] David Galindo, Sebastià Martín Molleví, Paz Morillo, and Jorge Luis Villar. Easy verifiable primitives and practical public key cryptosystems. In Colin Boyd and Wenbo Mao, editors, *ISC 2003*, volume 2851 of *LNCS*, pages 69–83. Springer, October 2003.

[15] Craig Gentry. Practical identity-based encryption without random oracles. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 445–464. Springer, May / June 2006.

[16] Craig Gentry and Shai Halevi. Hierarchical identity based encryption with polynomially many levels. In Omer Reingold, editor, *TCC 2009*, volume 5444 of *LNCS*, pages 437–456. Springer, March 2009.

[17] Jens Groth and Amit Sahai. Efficient non-interactive proof systems for bilinear groups. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 415–432. Springer, April 2008.

[18] Dennis Hofheinz and Tibor Jager. Tightly secure signatures and public-key encryption. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 590–607. Springer, August 2012.

[19] Allison B. Lewko. Tools for simulating features of composite order bilinear groups in the prime order setting. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 318–335. Springer, April 2012.

[20] Benoît Libert, Marc Joye, Moti Yung, and Thomas Peters. Concise multi-challenge CCA-secure encryption and signatures with almost tight security. In *Proceedings of ASIACRYPT 2014*, Lecture Notes in Computer Science. Springer, 2014.

[21] Brent Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple as-

sumptions. In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 619–636. Springer, August 2009.