Chosen-Ciphertext Secure Identity-Based Encryption in the Standard Model with short Ciphertexts

Eike Kiltz

CWI Amsterdam
kiltz@cwi.nl

Abstract

We describe a practical identity-based encryption scheme that is secure in the standard model against chosen-ciphertext (IND-CCA2) attacks. Security is based on an assumption comparable to (but slightly stronger than) Bilinear Decisonal Diffie-Hellman (BDDH). A comparison shows that our construction outperforms all known identity-based encryption schemes in the standard model and its performance is even comparable with the one from the random-oracle based Boneh/Franklin IBE scheme. Our proposed IBE scheme has furthermore the property that it fulfills some notion of "redundancy-freeness", i.e. the encryption algorithm is not only a probabilistic injection but also a surjection. As a consequence the ciphertext overhead is nearly optimal: to encrypt k bit messages for k bit identities and with k bit randomness we get $3k$ bit ciphertexts to guarantee (roughly) k bits of security.

Keywords: Chosen-ciphertext security, Identity-Based Encryption, Bilinear Maps.

1 Introduction

Identity-Based Encryption. An Identity-Based Encryption (IBE) scheme is a public-key (asymmetric) encryption scheme where any string such as email addresses, server names or phone numbers, can be used as public keys. The ability to use identities as public keys largely reduces the need for public key certificates and certificate authorities to distribute public key certificates.

After Shamir proposed the concept of IBE in 1984 [41] it remained an open problem for almost two decades to come up with a satisfying construction for it. In 2001, Boneh and Franklin [9] proposed formal security notions for IBE systems and designed a fully functional secure IBE scheme using bilinear maps. This scheme and the tools developed in its design have been successfully applied in numerous cryptographic settings, transcending by far the identity based cryptography framework. Though reletively recent invented IBE is already intensively applied in practice (see, e.g., http://www.voltage.com). Furtheremore, IBE is currently in the process of getting standardized — from February 2006 on the new IEEE P1363.3 standard for "Identity-Based Cryptographic Techniques using Pairings" [28] accepts submissions.

An alternative but less efficient IBE construction was proposed by Cocks [18] based on quadratic residues. Both IBE schemes provide security against *chosen-ciphertext attacks* (through Fujisaki-Okamoto [21]). In a chosen ciphertext attack, the adversary is given access to a decryption oracle that allows him to obtain the decryptions of ciphertexts of his choosing. Intuitively, security in this setting means that an adversary obtains (effectively) no information about encrypted messages, provided the corresponding ciphertexts are never submitted to the decryption oracle. For different reasons, the notion of chosen-ciphertext security has emerged as the "right" notion of security for encryption schemes. We stress that, in general, chosen-ciphertext security is a much stronger security requirement than chosen-plaintext attacks [2], where in the latter an attacker is not given access to the decryption oracle.

The drawback of the IBE scheme from Boneh-Franklin and Cocks is that security can only be guaranteed in the *random oracle* model [3], i.e. in an idealized world where all parties magically get black-box access to a truly random function. Unfortunately a proof in the random oracle model can only serve as a heuristic argument and has proved to possibly lead to insecure schemes when the random oracles are implemented in the standard model (see, e.g., [12]).

Waters' IBE. To fill this gap Waters [43] presents the first efficient Identity-Based Encryption scheme that is chosen-plaintext secure without random oracles. The proof of his scheme makes use of an algebraic method first used by Boneh and Boyen [6] and security of the scheme is based on the Bilinear Decisional Diffie-Hellman (BDDH) assumption. However, Waters' plain IBE scheme only guarantees security against passive adversaries (chosen-plaintext security).

From 2-level Hierarchical IBE to chosen-chipertext secure IBE. Hierarchical identity-based encryption (HIBE) [27, 22] is a generalization of IBE allowing for hierarchical delegation of decryption keys. Recent results from Canetti, Halevi, and Katz [13], further improved upon by Boneh and Katz [10] show a generic and practical transformation from any chosen-plaintext secure 2-level HIBE scheme to a chosen-ciphertext secure IBE scheme. Since Waters' IBE scheme can naturally be extended to a 2-level HIBE this implies the first efficient chosen-ciphertext secure IBE in the standard model. Key size, as well as the security reduction of the resulting scheme are comparable to the ones from Waters' IBE. However, the transformation involves some symmetric overhead to the ciphertext in form of a one-time signature or a MAC with their respective keys.

The first "direct" (non 2-level HIBE based) chosen-ciphertext IBE construction in the standard model was mentioned by Boyen, Mei, and Waters [11] and later improved by Galindo and Kiltz [29]. Both constructions are based on Waters' IBE and add one additional element to the ciphertext that is used for a consistency check in the decryption algorithm. However, in terms of ciphertext size and performance it did not introduce a dramatic improvement over the generic 2-level HIBE based constructions.

Identity-based key encapsulation. Instead of providing the full functionality of an IBE scheme, in many applications it is sufficient to let sender and receiver agree on a common random session key. This can be accomplished with an *identity-based key encapsulation mechanism* (IB-KEM) as formalized in [20, 5]. Any IB-KEM can be updated to a full IBE scheme by adding a symmetric encryption scheme. The latter one is also called a data encapsulation scheme (DEM) and the resulting identity-based encryption scheme the resulting hybrid IBE scheme. If both the IB-KEM and the DEM are chosen-ciphertext secure, then the hybrid IBE scheme is also chosen-ciphertext secure. We note that chosen-ciphertext secure DEMs can be created from relatively weak primitives such as a one-time symmetric encryption scheme (e.g., a one-time pad) plus a message authentication code (MAC). In the public-key setting most standards are given in terms of KEM primitives and we find it very likely that the upcoming IEEE P1363.3 standard [28] will also follow this principle. We therefore decided to focus in this paper on IB-KEM's only.

1.1 Our Contributions

A new chosen-ciphertext secure IB-KEM/IBE scheme. Based on Waters' chosen-plaintext secure IBE scheme we present a new and direct identity-based key encapsulation mechanism with short ciphertexts and very efficient encapsulation/decapsulation algorithms. Chosen-ciphertext security is obtained at sheer optimal cost. Compared to Waters' raw chosen-plaintext secure IBE scheme (viewed as an IB-KEM) our scheme comes with the same ciphertext overhead whereas computational overhead is one more exponentiation for encapsulation and two more exponentiations for decapsulation. We give a rigorous game-based proof reducing chosen-ciphertext security of our scheme to breaking the *modified Bilinear Decisional Diffie-Hellman assumption* (mBDDH), an assumption closely related to BDDH. By adding a one-time secure symmetric encryption scheme and a MAC we obtain a new hybrid IBE scheme with short ciphertexts using the IB-KEM/DEM methodology [5].

An identity-preserving redundancy-free IBE scheme in the standard model. It is furthermore possible to obtain a full IBE scheme with shorter ciphertexts by using the DEMs based on the CMC [25] and EME [26] mode of operation that avoid the overhead due to the MAC. Then ciphertexts of our IBE come with minimal overhead, i.e they are *identity-preserving redundancy-free.* Following Phan and Pointcheval [37] this property means that the IBE encryption algorithm (viewed as a mapping from randomness space, identity space, and message space into the ciphertext space) is a bijection. Consequently all possible ciphertexts in the ciphertext space are reachable by the encryption algorithm — shrinking the ciphertext any further is not possible. Our construction is the first weakly redundancy-free IBE scheme in the standard model.

A (stronger) notion of redundancy-free IBE schemes further requires that even *for any possible identity* from the identity-space the encryption algorithm (now viewed as a mapping from randomness space and message space into the ciphertext space) is a bijection. Obtaining such strongly redundancy-free IBE schemes is possible but they are only known to exist in the random oracle model and under the highly non-standard "gap-BDDH" assumption [31].

We find even the existence of identity-preserving redundancy-free IBE schemes in the standard model particularly remarkable since in the standard public-key encryption setting redundancy-free schemes (in the sense of [37]) are not known to exist. We further remark that the ciphertexts of our IBE scheme have the same message expansion as the most efficient standard public-key encryption schemes (like Kurosawa/Desmedt [30] and BMW [11]), i.e. compared to standard PKE we obtain identity-based encryption with no overhead.

The mBDDH assumption and its relation to known assumptions. As a by-product we formalize and study our new mBDDH assumption and relate its hardness to well-known pairing-based "standard assumptions". In particular we show that "2-BDDHI is at least as strong as mBDDH is at least as strong as BDDH". The 2-BDDHI (2 Biliear Decisional Diffie-Hellman Inversion) assumption was introduced by Boneh and Boyen [6] and its stronger variants (q-BDDHI for some polynomial q) already found numerous applications in [6, 7, 8, 35].

1.2 Related Work and Comparison

In [11] it was shown how to use "identity-based techniques" from [13] to obtain direct chosen-ciphertext secure public-key encryption schemes. The techniques from [11] basically rely on combining [13] with a tick orginally due to Cramer and Shoup [19] to use a (target collision resistant) hash function to "tie" some elements of ciphertexts together. As we already pointed out, chosen-ciphertext secure IBE scheme were known to exist using generic reductions [13] based on Waters' 2-level HIBE [43]. The first direct chosen-ciphertext secure IBE scheme was mentioned in [11]. Improving on the results from [11] the first concrete full construction with a formal security proof was provided in [29]. The latter scheme can be seen as combining the 2-level HIBE scheme obtained from Waters' IBE at the first level and Boneh-Boyen [6] at the second level with the "direct chosen-ciphertext secure techniques" from [11] to obtain a direct chosen-ciphertext secure IBE scheme. Compared to Waters' chosen-plaintext secure IBE scheme, the latter direct construction adds one additional redundant element to the ciphertext. Like in the construction from [11] this element is used as a "check" to defend against invalid ciphertexts, where the check had to be carried out using bilinear pairings. A similar validity check is implicitly contained in the generic constructions based on 2-level HIBEs [13].

The main idea of our new scheme is to encode the information necessary for the validity check into Waters' original ciphertext. More precisely, we were able to encode the consistency information in ciphertext element containing the reciever's idenity. This more efficient encoding also enables us to perform a more efficient decryption. In a broader view our new scheme can also be seen as combining the 2-level HIBE scheme obtained using the construction from Boneh-Boyen-Go [8] with Waters' IBE at the first level and Boneh-Boyen [6] at the second level, with some variant of the techniques from [11] to obtain a direct chosen-ciphertext secure IBE scheme. However, we want to stress that it is not obvious if the Boneh-Boyen-Go [8] HIBE can be instanciated with Waters' technique to get a fully secure HIBE scheme, similar to the one described above. Nor if the technique of [19, 11] can be applied to the latter construction to obtain a direct chosen-ciphertext secure IBE scheme. In some sense out results answer the two above questions to the positive. However, we think that our specific scheme and in particular its proof of security are not self-evident given the state of our knowledge in this area. In this context we want to repeat again that unlike the construction given in [11] our direct chosen-ciphertext technique does not expand the ciphertext by one element. Unfortunately it does not seem to be aplicable to the original public-key setting to obtain shorter ciphertexts in [11].

A comparison with chosen-ciphertext secure IBE schemes in the standard model. We will (in Section 7) carefully review all known chosen-ciphertext secure IBE constructions, including the above proposals, and make an extensive comparison with our scheme. In terms of ciphertext expansion our IBE scheme saves (at least) one group element compared to all so far known constructions, which makes a relative saving of 33% (i.e., two instead of three elements). The relative savings for encryption/decryption are (at least) one exponentiation and one pairing plus one exponentiation, respectively which again sums up to a relative saving of (roughly) 33%. We conclude that, to the best of our knowledge, the proposed IBE scheme is the most efficient chosen-ciphertext secure IBE scheme in the standard model.

A comparison with the Boneh/Franklin random oracle IBE scheme. Using recent experimental data for atomic primitives (such as exponentiations and pairings) from Granger, Page, and Smart [24] we estimate the efficiency of a possible implementation of our scheme using asymmetric pairings over non-singular elliptic curves. We make a careful comparison at various practical security levels with the only IBE scheme that is currently employed in practise: the IBE scheme from Boneh and Franklin [9], which is only known to be secure in the random oracle model. In turns out that the efficiency of our scheme is comparable to the one from Boneh and Franklin — ciphertext expansion is more or less the same and encryption is a factor of 3 to 10 faster (depending on the chosen security parameter), whereas decryption is about 1.5 to 3 times slower. We conclude that our scheme has ciphertext size and efficiency comparable to the random oracle based Boneh/Franklin IBE scheme.

2 Definitions

2.1 Notation

If x is a string, then $|x|$ denotes its length, while if S is a set then $|S|$ denotes its size. If $k \in \mathbb{N}$ then 1^k denotes the string of k ones. If S is a set then $s \stackrel{\$}{\leftarrow} S$ denotes the operation of picking an element s of S uniformly at random. We write $\mathcal{A}(x, y, \ldots)$ to indicate that $\mathcal{A}$ is an algorithm with inputs $x, y, \ldots$ and by $z \stackrel{\$}{\leftarrow} \mathcal{A}(x, y, \ldots)$ we denote the operation of running $\mathcal{A}$ with inputs $(x, y, \ldots)$ and letting z be the output. We write $\mathcal{A}^{\mathcal{O}_1, \mathcal{O}_2, \cdots}(x, y, \ldots)$ to indicate that $\mathcal{A}$ is an algorithm with inputs $x, y, \ldots$ and access to oracles $\mathcal{O}_1, \mathcal{O}_2, \ldots$ and by $z \stackrel{\$}{\leftarrow} \mathcal{A}^{\mathcal{O}_1, \mathcal{O}_2, \cdots}(x, y, \ldots)$ we denote the operation of running $\mathcal{A}$ with inputs $(x, y, \ldots)$ and access to oracles $\mathcal{O}_1, \mathcal{O}_2, \ldots$, and letting z be the output.

2.2 Secure Identity Based Key Encapsulation

An *identity-based key-encapsulation mechanism* (IB-KEM) scheme [41, 9] $\mathcal{IBKEM} = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{Encaps}, \mathsf{Decaps})$ consists of four polynomial-time algorithms. Via $(pk, msk) \xleftarrow{\$} \mathsf{Setup}(1^k)$ the randomized key-generation algorithm produces master keys for security parameter $k \in \mathbb{N}$; via $usk[id] \xleftarrow{\$} \mathsf{Extract}(msk, id)$ the master computes the secret key for identity id; via $(C, K) \xleftarrow{\$} \mathsf{Encaps}(pk, id)$ a sender creates a random session key K and a corresponding ciphertext C with respect to identity id; via $K \leftarrow \mathsf{Decaps}(usk, C)$ the possessor of secret key usk decapsulates ciphertext C to get back a session key K. Associated to the scheme is a key space KeySp. For consistency, we require that for all $k \in \mathbb{N}$, all identities id, and all $(C, K) \xleftarrow{\$} \mathsf{Encaps}(pk, id)$, we have $\Pr[\mathsf{Decaps}(\mathsf{Extract}(msk, id), C) = K] = 1$, where the probability is taken over the choice of $(pk, msk) \xleftarrow{\$} \mathsf{Setup}(1^k)$, and the coins of all the algorithms in the expression above.

The strongest and commonly accepted notion of security for an indentity-based key encapsulation scheme is that of *indistinguishability against an adaptive chosen ciphertext attack.* This notion, denoted IND-CCA, is defined using the following game between a challenger and an adversary $\mathcal{A}$. Let $\mathcal{IBKEM} = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{Encaps}, \mathsf{Decaps})$ be an IB-KEM with associated key space KeySp. To an adversary $\mathcal{A}$ we associate the following experiment:

```
Experiment $\mathbf{Exp}^{\mathrm{cca}}_{\mathcal{IBKEM},\mathcal{A}}(k)$
    $(pk, msk) \xleftarrow{\$} \mathsf{Setup}(1^k)$
    $(id^*, state) \xleftarrow{\$} \mathcal{A}^{\textsc{Extract}(\cdot),\textsc{Decaps}(\cdot,\cdot)}(\mathtt{find}, pk)$
    $K_0^* \xleftarrow{\$} \mathsf{KeySp}$ ; $(C^*, K_1^*) \xleftarrow{\$} \mathsf{Encaps}(pk, id^*)$
    $\gamma \xleftarrow{\$} \{0,1\}$ ; $K^* \leftarrow K_\gamma^*$
    $\gamma' \xleftarrow{\$} \mathcal{A}^{\textsc{Extract},\textsc{Decaps}}(\mathtt{guess}, K^*, C^*, state)$
    If $\gamma \neq \gamma'$ then return 0 else return 1
```

The oracle $\textsc{Extract}(id)$ returns $sk[id] \xleftarrow{\$} \textsc{Extract}(msk, id)$ with the restriction that $\mathcal{A}$ is not allowed to query oracle $\textsc{Extract}(\cdot)$ for the target identity id^*. The oracle $\textsc{Decaps}(id, C)$ first computes $sk[id] \xleftarrow{\$} \textsc{Extract}(msk, id)$ as above and then returns $K \leftarrow \mathsf{Decaps}(sk[id], id, C)$ with the restriction that in the guess stage $\mathcal{A}$ is not allowed to query oracle $\textsc{Decaps}(\cdot, \cdot)$ for the tuple (id^*, C^*). *state* is some internal state information of adversary $\mathcal{A}$ and can be any (polynomially bounded) string. We define the advantage of $\mathcal{A}$ in the chosen-ciphertext experiment as

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathcal{IBKEM},\mathcal{A}}(k) \;=\; \left| \Pr\left[\mathbf{Exp}^{\mathrm{cca}}_{\mathcal{IBKEM},\mathcal{A}}(k) = 1 \right] - \frac{1}{2} \right| .$$

An IB-KEM $\mathcal{IBKEM}$ is said to be *secure against chosen-ciphertext attacks* (CCA secure) if the advantage functions $\mathbf{Adv}^{\mathrm{cca}}_{\mathcal{IBKEM},\mathcal{A}}(k)$ is a negligible function in k for all polynomial-time adversaries $\mathcal{A}$.

We remark that our security definition is given with respect to "full-identity" attacks, as opposed to the much weaker variant of "selective-identity" attacks where the adversary has to commit to its target identity id^* in advance, even before seeing the public key.

2.3 Target Collision Resistant Hash Functions

Let $\mathcal{F} = (\mathsf{TCR}_s)_{s \in S}$ be a family of hash functions for security parameter k and with seed $s \in S = S(k)$. $\mathcal{F}$ is said to be *collision resistant* if, for a hash function $\mathsf{TCR} = \mathsf{TCR}_s$ (where the seed is chosen at random from S), it is infeasible for an efficient adversary to find two distinct values $x \neq y$ such that $\mathsf{TCR}(x) = \mathsf{TCR}(y)$.

A weaker notion is that of *target collision resistant hash functions.* Here it should be infeasible for an efficient adversary to find, given a randomly chosen element x and a randomly drawn hash function

$\mathsf{TCR} = \mathsf{TCR}_s$, a distinct element $y \neq x$ such that $\mathsf{TCR}(x) = \mathsf{TCR}(y)$. (In collision resistant hash functions the value x may be chosen by the adversary.) Such hash functions are also called *universal one-way hash functions* [34] and can be built from arbitrary one-way functions [34, 38]. We define (slightly informal)

$$\mathbf{Adv}^{\text{hash-tcr}}_{\mathsf{TCR},\mathcal{H}}(k) = \Pr[\mathcal{H} \text{ finds a collision in } \mathsf{TCR}].$$

Hash function family is said to be a *target collision resistant* if the advantage function $\mathbf{Adv}^{\text{hash-tcr}}_{\mathsf{TCR},\mathcal{H}}$ is a negligible function in k for all polynomial-time adversaries $\mathcal{H}$.

In practice, to build a target collision resistant hash function TCR, one can use a dedicated cryptographic hash function, like SHA-1 [40]. For that reason and to simplify our presentation, in what follows we will consider the hash function TCR to be a fixed function.

3 Assumptions

3.1 Parameter generation algorithms for Bilinear Groups.

All pairing based schemes will be parameterized by a *pairing parameter generator*. This is a PTA $\mathcal{G}$ that on input 1^k returns the description of an multiplicative cyclic group $\mathbb{G}$ of prime order p, where $2^k < p < 2^{k+1}$, the description of a multiplicative cyclic group $\mathbb{G}_T$ of the same order, and a non-degenerate bilinear pairing $\hat{e}$: $\mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. See [9] for a description of the properties of such pairings. We use $\mathbb{G}^*$ to denote $\mathbb{G} \setminus \{1\}$, i.e. the set of all group elements except the neutral element. Throughout the paper we use $\mathcal{PG} = (\mathbb{G}, \mathbb{G}_T, p, \hat{e}, g)$ as shorthand for the description of bilinear groups, where g is a generator of $\mathbb{G}$.

3.2 The modified BDDH assumption

Let $\mathcal{PG}$ be the description of pairing groups. Consider the following problem: Given $(g, g^a, g^b, g^{(b^2)}, g^c, W) \in \mathbb{G}^5 \times \mathbb{G}_T$ as input, output yes if $W = \hat{e}(g,g)^{abc}$ and no otherwise. The mBDDH assumption states that, roughly, this problem is computational infeasible. Note that this is nearly the standard BDDH assumption (see Appendix C for a formal definition) with the only difference that with mBDDH a distinguisher is additionally provided with the element $g^{(b^2)}$ (which is hard to compute from g^b).

More formally, to a parameter generation algorithm for pairing-groups $\mathcal{G}$ and an adversary $\mathcal{B}$ we assotiate the following experiment.

```
**Experiment** $\mathbf{Exp}^{\text{mbddh}}_{\mathcal{G},\mathcal{B}}(1^k)$
    $\mathcal{PG} \xleftarrow{\$} \mathcal{G}(1^k)$
    $a, b, c, w \xleftarrow{\$} \mathbb{Z}_p^*$
    $\beta \xleftarrow{\$} \{0,1\}$. If $\beta = 1$ then $W \leftarrow \hat{e}(g,g)^{abc}$ else $W \leftarrow \hat{e}(g,g)^w$
    $\beta' \xleftarrow{\$} \mathcal{B}(1^k, \mathcal{PG}, g, g^a, g^b, g^{b^2}, g^c, W)$
    If $\beta \neq \beta'$ then return 0 else return 1
```

We define the advantage of $\mathcal{B}$ in the above experiment as

$$\mathbf{Adv}^{\text{mbddh}}_{\mathcal{G},\mathcal{B}}(k) \;=\; \left| \Pr\left[\mathbf{Exp}^{\text{mbddh}}_{\mathcal{G},\mathcal{B}}(1^k) = 1 \right] - \frac{1}{2} \right| \, .$$

We say that the *modified Bilinear Decision Diffie-Hellman (mBDDH) assumption relative to generator* $\mathcal{G}$ holds if $\mathbf{Adv}^{\text{mbddh}}_{\mathcal{G},\mathcal{B}}$ is a negligible function in k for all PTAs $\mathcal{B}$.

3.3 Relation to BDDH and q-BDDHI

The next lemma classifies the strength of the modified BDDH assumption we introduced between the well known *standard pairing-based assumptions* BDDH and 2-BDDHI (see Appendix C for definitions). Here "A $\leq$ B" means that assumption B implies assumption A (in a black-box sense), i.e. assumption B is a stronger assumption than A.

Lemma 3.1 BDDH $\leq$ mBDDH $\leq$ 2-BDDHI $\leq$ 3-BDDHI $\leq \dots$

The simple proof is postponed until Appendix C.3. Since 2-BDDHI is known to hold in the generic-group model [7] this in particular implies correctness of the mBDDH assumption in generic-groups.

4 A chosen-ciphertext secure IB-KEM based on mBDDH

In this section we present our new chosen-ciphertext secure IB-KEM. Let $\mathcal{PG} = (\mathbb{G}, \mathbb{G}_T, p, \hat{e}, g)$ be public system parameters obtained by running the group parameter algorithm $\mathcal{G}(1^k)$.

4.1 Waters' Hash

We review the hash function $\mathsf{H} : \{0,1\}^n \to \mathbb{G}$ used in Waters' identity based encryption schemes [43]. On input of an integer n, the randomized hash key generator $\mathsf{HGen}(\mathbb{G})$ chooses $n+1$ random group elements $h_0, \dots, h_n \in \mathbb{G}$ and returns $h = (h_0, h_1, \dots, h_n) \in \mathbb{G}^{n+1}$ as the public description of the hash function. The hash function $\mathsf{H} : \{0,1\}^n \to \mathbb{G}^*$ is evaluated on a string $id = (id_1, \dots, id_n) \in \{0,1\}^n$ as the product

$$\mathsf{H}(id) = h_0 \prod_{i=1}^{n} h_i^{id_i} \in \mathbb{G}.$$

In Appendix D.1 we remind the reader of Water's original chosen-plaintext secure IBE scheme.

4.2 The IB-KEM Construction

Let $\mathsf{TCR} : \mathbb{G} \to \mathbb{Z}_p$ be a target collision-resistant hash function (whose definition can be looked up in Appendix 2.3). Our IB-KEM with identity space $\mathsf{IDSp} = \{0,1\}^n$ ($n = n(k)$) and key space $\mathsf{KeySp} = \mathbb{G}_T$ is depicted in Figure 1.

We call a (possibly malformed) ciphertext $C = (c_1, c_2) \in \mathbb{G}^2$ *consistent* (w.r.t identity id and public key pk) if $(g, c_1, \mathsf{H}(id) \cdot u^t, c_2)$ is a Diffie-Hellman tuple[1], where $t = \mathsf{TCR}(c_1)$. A correctly generated ciphertext for identity id has the form $C = (c_1, c_2) = (g^r, (\mathsf{H}(id) \cdot u^t)^r)$ and therefore $(g, c_1, \mathsf{H}(id) \cdot u^t, c_2) = (g, c_1, \mathsf{H}(id) \cdot u^t, (\mathsf{H}(id) \cdot u^t)^r)$ is always a DH tuple and consequently C is consistent. Testing for a DH-tuple is equivalent to checking if if $\hat{e}(g, c_2) = \hat{e}(\mathsf{H}(id) \cdot u^t, c_1)$ and therefore consistency of C can be implemented by evaluating the bilinear map twice. Note that this consistency test can be performed by anybody knowing the public-key only. This property is called "public verification" of the ciphertext.

4.3 Alternative Decapsulation

We now describe an alternative deterministic decapsulation algorithm which is more intuitive but less efficient. We claim that the decapsulation algorithm from Figure 1 is equivalent to

1. Compute $t = \mathsf{TCR}(c_1)$ and check if $(g, c_1, \mathsf{H}(id) \cdot u^t, c_2)$ is a DH tuple. If not, a random session key

[1] A tuple $(g, g^a, g^b, g^c) \in \mathbb{G}^4$ is said to be a *Diffie-Hellman tuple* (DH tuple)i f $ab = c \bmod p$.

```
Setup($1^k$)
    $\alpha, u \xleftarrow{\$} \mathbb{G}^*$ ; $z \leftarrow \hat{e}(g, \alpha)$
    $\mathsf{H} \xleftarrow{\$} \mathsf{HGen}(\mathbb{G})$
    $mpk \leftarrow (\mathsf{H}, u, z) \in \mathbb{G}^{n+2} \times \mathbb{G}_T$ ; $msk \leftarrow \alpha \in \mathbb{G}$
    Return $(mpk, msk)$
```

```
Extract($msk, id$)
    $s \xleftarrow{\$} \mathbb{Z}_p$
    $sk[id] \leftarrow (\alpha \cdot \mathsf{H}(id)^s, g^s, u^s) \in \mathbb{G}^3$
    Return $sk[id]$
```

```
Encaps($mpk, id$)
    $r \xleftarrow{\$} \mathbb{Z}_p^*$
    $c_1 \leftarrow g^r$ ; $t \leftarrow \mathsf{TCR}(c_1)$
    $c_2 \leftarrow (\mathsf{H}(id) \cdot u^t)^r$
    $K \leftarrow z^r \in \mathbb{G}_T$
    $C \leftarrow (c_1, c_2) \in \mathbb{G}^2$
    Return $(C, K)$
```

```
Decaps($mpk, id, sk[id], C$)
    Parse $C$ as $(c_1, c_2)$
    Parse $sk[id]$ as $(d_1, d_2, d_3)$
    $t \leftarrow \mathsf{TCR}(c_1)$
    $v \xleftarrow{\$} \mathbb{Z}_p^*$
    Return $K \leftarrow \frac{\hat{e}(d_1 \cdot d_3^t \cdot (\mathsf{H}(id)u^t)^v, c_1)}{\hat{e}(g^v \cdot d_2, c_2)}$
```

Figure 1: Our chosen-ciphertext secure identity-based key encapsulation.

K is returned (or the ciphertext gets rejected).
2. Otherwise return $K \leftarrow \hat{e}(c_1, d_1 \cdot d_3^t)/\hat{e}(c_2, d_2)$

To prove this claim we define the function $\Delta(C) = \hat{e}(c_1, \mathsf{H}(id)u^t)/\hat{e}(g, c_2)$. Then $\Delta(C) = 1$ if and only if C is consistent. Consequently, for a random $v \in \mathbb{Z}_p^*$, $K = \hat{e}(d_1 \cdot d_3^t, c_1)/\hat{e}(d_2, c_2) \cdot (\Delta(C))^v \in \mathbb{G}_T^*$ evaluates to $\hat{e}(d_1 \cdot d_3^t, c_1)/\hat{e}(d_2, c_2)$ if C is consistent and to a random group element otherwise. The claim then follows by

$$\begin{aligned} K &= \hat{e}(c_1, d_1 \cdot d_3^t)/\hat{e}(c_2, d_2) \cdot (\Delta(C))^v \\ &= \hat{e}(c_1, d_1 \cdot d_3^t)/\hat{e}(c_2, d_2) \cdot (\hat{e}(c_1, \mathsf{H}(id)u^t)/\hat{e}(g, c_2))^v \\ &= \frac{\hat{e}(c_1, d_1 \cdot d_3^t \cdot (\mathsf{H}(id)u^t)^v)}{\hat{e}(c_2, g^v \cdot d_2)} . \end{aligned}$$

We remark that the original decapsulation algorithm roughly saves two pairing operations.

We now show correctness of the scheme, i.e. that the K computed in the encapsulation algorithm matches the key K computed in the alternative decapsulation algorithm. We already showed that a correctly generated ciphertext is always consistent. A correctly generated secret key for identity id has the form $sk[id] = (d_1, d_2, d_3) = (\alpha \cdot \mathsf{H}(id)^s, g^s, u^s)$. Therefore the key decryption algorithm computes the key K as

$$\begin{aligned} K &= \hat{e}(c_1, d_1 \cdot d_3^t)/\hat{e}(c_2, d_2) \\ &= \hat{e}(g^r, \alpha\mathsf{H}(id)^s \cdot (u^s)^t)/\hat{e}((\mathsf{H}(id) \cdot u^t)^r, g^s) \\ &= \hat{e}(g^r, \alpha) \cdot \hat{e}(g^r, \mathsf{H}(id)^s \cdot (u^s)^t)/\hat{e}((\mathsf{H}(id) \cdot u^t)^r, g^s) \\ &= z^r \cdot \hat{e}(g^r, (\mathsf{H}(id) \cdot u^t)^s)/\hat{e}((\mathsf{H}(id) \cdot u^t)^s, g^r) \\ &= z^r, \end{aligned}$$

as the key computed in the encryption algorithm. This shows correctness.

4.4 Security

Theorem 4.1 Assume TCR is a target collision resistant hash function. Under the modified Bilinear Decisional Diffie-Hellman (mBDDH) assumption relative to generator $\mathcal{G}$, the IB-KEM from Section 4.2

is secure against chosen-ciphertext attacks. In particular, we have

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathcal{IBKEM},\mathcal{A}} = \mathcal{O}(nq \cdot (\epsilon + q/p) + \mathbf{Adv}^{\text{hash-tcr}}_{\mathsf{TCR},\mathcal{H}}(k)) \ ,$$

for any adversary $\mathcal{A}$ running for time $\mathbf{Time}_{\mathcal{A}}(k) = \mathbf{Time}_{\mathcal{B}} - \Omega(\epsilon^{-2} \cdot \ln(\epsilon^{-1}) + q)$, where $\epsilon = \mathbf{Adv}^{\mathrm{mbddh}}_{\mathcal{G},\mathcal{B}}(k)$ and q is an upper bound on the number of key derivation/decryption queries made by adversary $\mathcal{A}$.

The proof of Theorem 4.1 uses ideas from Waters [43] and will be given in Appendix B.

5 (Redundancy-free) Identity-Based Encryption

In this section we present various (known) extensions of our IBE construction, some of them are crucical for its aplication. Given an IB-KEM and a symmetric encryption scheme, a hybrid identity-based encryption scheme can be obtained by using the IB-KEM to securely transport a random session key that is fed into the symmetric encryption scheme (also called data encapsulation mechanism — DEM) to encrypt the plaintext message. It was recently shown in [5] that if both the IB-KEM and the DEM are chosen-ciphertext secure, then the resulting hybrid encryption is also chosen-ciphertext secure. The security reduction is tight.

A DEM secure against chosen-ciphertext attacks can be built from relatively weak primitives, i.e. from any one-time symmetric encryption scheme by essentially adding a MAC. For concreteness we mention that a chosen-ciphertext secure IBE scheme can be built from our IB-KEM construction with an additional overhead of a DEM which consists of a (one-time secure) symmetric encryption plus additional 128 bits for the MAC.

The modes of operation CMC [25] and EME [26] both give chosen-ciphertext secure DEMs provided that the underlying block-cipher is a strong pseudorandom permutation and avoid the usual overhead due to the MAC.

We note that for the natural task of securely generating a joint random session key, a IB-KEM is sufficient and a fully-fledged identity-based encryption scheme is not needed.

At an abstract level, for each identity id from identity space IDSp, an IBE encryption algorithm IBEenc_{id} can be viewed as an injective mapping

$$\mathsf{IBEenc}_{id} : \mathsf{RandSp} \times \mathsf{MsgSp} \hookrightarrow \mathsf{CipherSp},$$

where RandSp is the randomness space, MsgSp is the message space, and $\mathsf{CipherSp}$ is the ciphertext space. For each identity $id \in \mathsf{IDSp}$ this mapping must be injective since otherwise reconstruction of the message $M \in \mathsf{MsgSp}$ (decryption) is not unique. That also implies that decrypting a fixed ciphertext with respect to different identities must consequently lead to distinct plaintexts. By our security definition we need a sufficiently large randomness space since otherwise the IBE scheme is not even indistinguishable against chosen-plaintext attacks [23]. Following Phan and Pointcheval [37] we say that an IBE scheme is *redundancy-free* if for any possible identity id the above encryption mapping IBEenc_{id} is a bijection, i.e. if all elements from the ciphertext space are “reachable”. This redundancy-free property means that in some sense the ciphertexts are minimal and can’t be further shrunk.

Our scheme only satisfies redundancy-freeness with respect to a different (weaker) notion, it is *identity-preserving redundancy-free* in the sense that the mapping

$$\mathsf{IBEenc} : \mathsf{RandSp} \times \mathsf{IDSp} \times \mathsf{MsgSp} \to \mathsf{CipherSp}$$

is a bijection, i.e. information about the identity id is absorbed by the ciphertext $\mathsf{CipherSp}$. This relaxation is useful if an IBE ciphertext is needed to be verifiable, i.e. if one can (publicly) verify if an IBE ciphertext was indeed encrypted with some given identity. Applications of this property can be found, e.g., in threshold IBE schemes [29]. It is easy to argue that IBE schemes that are identity-preserving redundancy-free are optimal among all schemes that are (publicly) verifiable (this is since the identity has to be somehow encoded in the ciphertext).

Using the IB-KEM/DEM paradigm with our IB-KEM constriction and one of the DEMs based on the CMC/EME mode of operation we get an identity-preserving redundancy-free chosen-ciphertext secure IBE scheme that is publicly verifiable.

As a consequence the ciphertext overhead of our IBE scheme is optimal with respect to the verifiability property. Suppose an adversary attacking the IBE scheme makes at most q decryption/key derivation queries. A common estimate used here is $q = 2^{30}$ (suggested by Bellare and Rogaway [4]). According to Theorem 4.1, to encrypt k bit messages for $n = k$ bit identities and with k bit randomness we get $3k$ bit ciphertexts to guarantee $\approx k - 30$ bits of security. The $30 = \log(q)$ bits of loss in the security stems from the fact that the security reduction in Theorem 4.1 is not optimal (and depends multiplicatively on q). We remark that the ciphertext size of our IBE scheme is about the same as the one of the most efficient (standard) public-key encryption schemes in the standard model [30, 11].

We mention that there exists a redundancy-free IBE scheme [31] (in the sense of the first definition) in the random oracle model but it's security proof depends on a highly non-standard assumption.[2]

6 Extensions

6.1 A Tradeoff between Public Key Size and Security Reduction and Arbitrary identities

As independently discovered in [14, 33], there exists an interesting trade-off between key-size of Waters' hash H and the security reduction of the IBE scheme.

The construction modifies Waters hash H as follows: Let the integer $l = l(k)$ be a new parameter of the scheme. In particular, we represent an identity $id \in \{0,1\}^n$ as an n/l-dimensional vector $id = (id_1, \ldots, id_{n/l})$, where each id_i is an l bit string. Waters hash is then redefined to $\mathsf{H} : \{0,1\}^n \to \mathbb{G}$, with $\mathsf{H}(id) = h_0 \prod_{i=1}^{n/l} h_i^{id_i}$ for random public elements $h_0, h_1, \ldots, h_{n/l} \in \mathbb{G}$. Waters' original hash function is obtained as the special case $l = 1$. It is easy to see that using this modification in our IBE scheme (i) reduces the size of the public key from $n + 3$ to $n/l + 3$ group elements, whereas (ii) it adds another multiplicative factor of 2^l to the security reduction of the IBE scheme (Theorem 4.1).[3]

Furthermore we want to remark that using a simple and well-known trick we can allow the idenity-space to contain arbitrary bitstrings by applying a collission resistant hash function $\mathsf{CR} : \{0,1\}^* \to \{0,1\}^n$ to the identities before applying Waters' hash.

For concreteness and for a scheme implemented in groups offering ≈ 80 bits of security we have $n = 160$ bits and therefore propose to use $l = 16$ or $l = 32$. This shrinks the public-key size to reasonable 10 or 5 group elements, respectively.

6.2 Chosen-ciphertext secure Hierarchical Identity-Based Encryption

Hierarchical identity-based encryption is a generalization of IBE to identities supporting hierarchical structures [27, 22]. By the relation to Waters IBE scheme it is easy to see that our technique can also be used to obtain a chosen-ciphertext secure HIBE. Using a technique from [8] it is furthermore

[2] The scheme in [31] is secure under the "gap-BDDH assumption" which is same as the BDDH assumption but it additionally assumes the existence of an efficient DDH algorithm in the target group $\mathbb{G}_T$ which is not known to exist.

[3] On the technical side our proof basically stays the same, only the bound from Lemma B.2 needs to be adapted to take the modified Waters' hash into account.

possible to reduce the HIBE ciphertext size to three elements, i.e. it is independent of the hierarchy's depth. As in [22, 43] the security reduction is only exponential in the depth d of the hierarchy, i.e. it introduces, roughly, a multiplicative factor of $(nq)^d$. The keysize of the HIBE scheme is $O(nd)$, whereas the same tradeoff between public-key size and security reduction mentioned in the last subsection is possible.

6.3 Selective-Identity Chosen-Ciphertext Secure IB-KEM

For the definition of a selective-identity chosen-ciphertext secure IB-KEM we change the security experiment such that the adversary has to commit to the target identity id^* before seeing the public key. Clearly, this is a weaker security requirement. We quickly note that (using an algebraic technique from [6]) by replacing Waters' hash H with $\mathsf{H}(id) = h_0 \cdot h_1^{id}$ (for $id \in \mathbb{Z}_p$) we get a selective-id chosen-ciphertext secure IB-KEM. Note that the size of the public-key of this scheme drops to 3 elements.

6.4 IB-KEM with Non-Interactive Threshold Decryption

Exploiting the public verifiability property of the ciphertext and using the same ideas as in [29] we are able to make key derivation and decapsulation of our IB-KEM construction "threshold". The ciphertexts of the resulting threshold IB-KEM are shorter in comparison with [29].

6.5 Chosen-Ciphertext Secure IB-KEM in the random oracle model

Replacing Water's hash H with $\mathsf{H}(id) = h_0 \cdot h_1^{\mathsf{R}(id)}$ (where $\mathsf{R} : \{0,1\}^* \to \mathbb{Z}_p$ is a random oracle) we get (using the slective-identity secure scheme from the last subsection and a general result from [6]) a chosen-ciphertext secure IB-KEM in the random oracle model. By adding another random oracle to the symmetric key the scheme can then be proved chosen-ciphertext secure with respect to the computation variant of the mBDDH assumption. Again the size of the public-key of this scheme drops to 3 elements.

6.6 Implementing the Target Collision Resistant Hash Function TCR

In practice, to build a target collision resistant hash function, one can use a dedicated cryptographic hash function, like SHA-1 [40]. Every injective function $\mathsf{TCR} : \mathbb{G} \to \mathbb{Z}_p$ trivially also is (target) collision resistant (with zero advantage). Boyen, Mei and Waters [11] note that for bilinear maps defined on elliptic curves there exists a very efficient way to implement such injective mappings. We refer to [11] for more details.

7 Comparison

In this section we compare our scheme with the known IBE schemes from the literature. For a uniform treatment we do all comparisons in terms of the respective IBE schemes. The previously most efficient CCA-secure IBE scheme is the one from Kiltz and Galindo [29]. We also compare our scheme with the generic construction [13] obtained from a 2-level HIBE [43, 6] and with the original (only chosen-plaintext secure) IBE scheme from Waters. Furthermore we compare or scheme with the reference random-oracle IBE scheme from Boneh and Franklin [9].

In pairing based cryptography efficiency depends on the chosen curve and how well the scheme can be adapted to it. Usually [13, 11] a comparison is done by taking the pairing as a black-box and under the simplified assumption that all exponentiations carried out in different groups have about the same running time. We will follow this approach in Section 7.1. Then, in Section 7.2 we will

Scheme	CCA	Standard	Size		Encrypt	Decrypt	Key Der.
	secure?	Model?	$\lvert C\rvert$	*pk*	#pairings +	#[multi,reg]-exp	
Ours+DEM	√	√	$2\lvert\mathbb{G}\rvert$+128	$n+3$	$0+[1,2]$	$2+[1,1]$	$0+[0,3]$
Kiltz/Galindo+DEM	√	√	$3\lvert\mathbb{G}\rvert$+128	$n+4$	$0+[1,3]$	$3+[1,3]$	$0+[0,2]$
Hybrid Waters/BB+CHK	√	√	$3\lvert\mathbb{G}\rvert$+768	$n+4$	$0+[1,3]$	$3+[1,2]$	$0+[0,2]$
(Waters)	—	√	$2\lvert\mathbb{G}\rvert$	$n+2$	$0+[0,3]$	$2+[0,0]$	$0+[0,2]$
(Boneh/Franklin)	√	—	$1\lvert\mathbb{G}\rvert$+256	1	$1+[0,2]$	$1+[0,1]$	$0+[0,1]$

Table 1: Efficiency comparison for chosen-ciphertext secure IBE schemes. Ciphertext overhead represents the difference (in bits) between the ciphertext length and the message length. The additional bits account for the necessary symmetric overhead for 128 bits security. The keysize of the public key is measured in terms of the number of group elements. The size of the secret key *sk* is the same for all three schemes (a single element in $\mathbb{G}$). For computational efficiency we neglect all symmetric operations (like symmetric encryption, random oracle hashes, and MACs). For comparison we mention that relative timings for the various operations are as follows: regular pairing $\approx 3-5$ [36], multi-exponentiation ≈ 1.5, regular exponentiation $= 1$.

discuss how our scheme can possibly be instantiated in non-supersingular asymmetric pairing groups. A carefull implementation-based comparison in the asymmetric setting with the Boneh/Franklin IBE scheme will then be done in Section 7.3.

7.1 Comparison in the symmetric setting

We will consider the following IBE schemes:

Ours+DEM: Our construction from Section 4 updated with a DEM to get a full IBE scheme.

Kiltz/Galindo+DEM: The IB-KEM from [29] updated with a DEM to get a full IBE scheme.

Hybrid Waters/BB+CHK: The IBE scheme obtained by the generic transformation [13, 10] applied to the 2-level hybrid HIBE consisting of Waters' IBE scheme [43] at the first level and the Boneh/Boyen IBE scheme [6] at the second level (as proposed in [43]).

Waters: Waters' plain chosen-plaintext secure IBE scheme [43].

Boneh/Franklin: The random-oracle "fullident" chosen-ciphertext secure IBE scheme [9].

Since evaluating Waters' hash H requires computing $n/2$ products in $\mathbb{G}$ on the average, where $n \leq \log_2 p$, it can be seen as a single exponentiation. Therefore we count computing $\mathsf{H}(id)^r$ for random r as two exponentiations in $\mathbb{G}$. For decryption the value $\mathsf{H}(id)$ can be precomputed (and assumed to be contained in $sk[id]$).

Comparison. An efficiency comparison is done in Table 1. We conclude that our scheme is the most efficient chosen-ciphertext secure IBE scheme in the standard model. Furthermore its performance and ciphertext expansion seems comparable to the random-oracle based reference scheme from Boneh/Franklin.

7.2 Our IBE scheme in asymmetric pairing groups

Our definition of the bilinear groups assumed a symmetric pairing $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. However, there is a large class of admissible bilinear groups which have an asymmetric pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, i.e. $\mathbb{G}_1 \neq \mathbb{G}_2$. Such asymmetric bilinear groups have the advantage of being less special than symmetric ones — and consequently have better security properties since their greater generality makes it harder to design tailor-made attacks. Furthermore, as we will sketch below, they can lead to considerably shorter ciphertexts than symmetric pairings.

Variant	Element ... in group					key decapsulation	Encryption	Decryption
	c_1	c_2	d_1	d_2	d_3		#pairings + #exp in $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$	
V1	$\mathbb{G}_2$	$\mathbb{G}_2$	$\mathbb{G}_1$	$\mathbb{G}_1$	$\mathbb{G}_1$	$\frac{\hat{e}(d_1 d_3^t (\mathsf{H}(id)u^t)^v, c_1)}{\hat{e}(g^v d_2, c_2)}$	$0 + (0, 3.5, 1)$	$1.5 + (2.5, 0, 0)$
V2	$\mathbb{G}_1$	$\mathbb{G}_1$	$\mathbb{G}_2$	$\mathbb{G}_2$	$\mathbb{G}_2$	$\frac{\hat{e}(c_1, d_1 d_3^t (\mathsf{H}(id)u^t)^v)}{\hat{e}(c_2, g^v d_2)}$	$0 + (3.5, 0, 1)$	$1.5 + (0, 2.5, 0)$
V3	$\mathbb{G}_2$	$\mathbb{G}_1$	$\mathbb{G}_1$	$\mathbb{G}_2$	$\mathbb{G}_1$	$\frac{\hat{e}(d_1 d_3^t (\mathsf{H}(id)u^t)^v, c_1)}{\hat{e}(c_2 g^v, d_2)}$	$0 + (2.5, 1, 1)$	$1.5 + (2.5, 0, 0)$

Table 2: Different asymmetric variants of our IBE scheme.

Variant	Ciphertext space	Ciphertext size	Encryption	Decryption
V1	$\mathbb{G}_2 \times \mathbb{G}_2$	big	slow	fast
V2	$\mathbb{G}_1 \times \mathbb{G}_1$	small	fast	slow
V3	$\mathbb{G}_2 \times \mathbb{G}_1$	big	medium	fast

Table 3: Tradeoff between ciphertext size and efficiency for our IBE variants.

In this setting we have to allocate the various group elements appearing in our IBE scheme to the two groups $\mathbb{G}_1$ and $\mathbb{G}_2$. Depending on how this is done we can give different trade-offs between computational efficiency for encryption/decryption and ciphertext size. To this end we will use the following conventions [24, 1]: (i) For general curves an element in $\mathbb{G}_2$ takes about α times as much space to represent as one in $\mathbb{G}_1$, where α (usually called k) is the embedding degree (typical values for α are $\alpha = 6, 12, 24$). In practise that means that elements in $\mathbb{G}_1$ have a small representation whereas elements in $\mathbb{G}_2$ not. (ii) An exponentiation in $\mathbb{G}_2$ takes about α as much time as an exponentiation in $\mathbb{G}_1$. We adapt the convention to count one multi-exponentiation as 1.5 exponentiations [13] and the ratio of two pairings as 1.5 pairings [11].[4] Based on those assumptions in Table 2 we give three variants of our IBE scheme with different tradeoffs between ciphertext size and encryption/decryption efficiency. The relative advantages are summarized in Table 3. We note that in case of asymmetric pairing groups the public key pk consists of $\mathbb{G}_c^{n+1} \times \mathbb{G}_T$, where $c = 2$ for variant 1 and $c = 1$ for variants 2 and 3 (i.e. the elements h_i and u have to be in the same group as the ciphertext element c_2). Therefore for variants 2 and 3 we can take benefit of the small representation in group G_1. We remark that some further care should be taken when instantiating pairing-based schemes in the asymmetric setting in a black-box way since due to the different premises the proof of security may not longer be valid. Indeed it is easy to verify that in our case the proofs are still valid for the three proposed variants.

7.3 A comparison with the Boneh/Franklin scheme in the asymmetric setting

In this section we demonstrate the practicability of our IBE scheme by comparing it with the one from Boneh/Franklin. We remark that the latter scheme is intensively used in practice (see, e.g., `http://www.voltage.com`). We aim to compare the schemes for fixed security parameters $k = 80, 128, 192, 256$. We denote the size of the message space by m.

Boneh/Franklin. We consider the fullident chosen-ciphertext secure Boneh/Franklin IBE scheme (which for completeness can be looked up in Appendix D.2). For encryption it performs one exponentiation in $\mathbb{G}_1$, one exponentiation in $\mathbb{G}_T$, one pairing, and one call a "hash-to-point" hash function $H_1 : \{0,1\}^n \to \mathbb{G}_2^*$, modeled as a random oracle. The latter one was already identified in [36, 16, 24] to be problematic to implement since one some curves it is not known to be efficiently implementable at

[4] Actually [11] mentions in Section 5.1 that "computation of a ratio of two pairings [...] can be done almost as efficiently as a single pairing, by modifying Miller's algorithm in a manner akin to multi-exponentiation [32]". We think that a factor of 1.5 is more realistic.

k	Curve $(\log_2 p, \alpha)$	Our IBE (Variant 2)			Our IBE (Variant 3)			Boneh/Franklin			Boneh/Franklin2		
		Enc	Dec	$\|C\|$	Enc	Dec	$\|C\|$	Enc	Dec	$\|C\|$	Enc	Dec	$\|C\|$
80	A (160,6)	4	20	400	8	10	720	16	6	320	11	10	640
128	B (512,6)	60	325	1152	115	187	2176	458	115	768	196	170	1792
128	C (256,12)	18	220	640	64	103	1920	314	66	512	118	113	1792
192	D (1365,6)	611	3687	2922	1170	2286	5652	7970	1431	1749	2472	1991	4479
192	E (683,12)	174	2405	1558	632	1259	4973	5472	815	1067	1350	1273	4482
256	F (2560,6)	2808	19074	5376	5386	12629	10496	51256	7989	3072	13613	10567	8192
256	G (1280,12)	788	11920	2816	2877	6697	9216	34950	4355	1792	6904	6445	8192
256	H (640,24)	262	7627	1536	1602	4276	8576	21418	2822	1152	4289	4163	8192

Table 4: Number of estimated 32 bit multiplications needed to perform Encryption/Decryption (scaled by 10^5) and ciphertext overhead in bits. The column $|C|$ gives the ciphertext overhead in bits.

all or it needs one "cofactor" exponentiation in $\mathbb{G}_2$. For decryption it needs one exponentiation in $\mathbb{G}_1$ and one pairing. The ciphertext space is $\mathbb{G}_1 \times \{0,1\}^{2k} \times \{0,1\}^m$, the $\{0,1\}^{2k}$ stems from the output of a hash function H_2 (due to the birthday attack a domain of $2k$ is needed to guarantee security of k bits).

Boneh/Franklin2. We denote by Boneh/Franklin2 the above scheme with switched roles of $\mathbb{G}_1$ and $\mathbb{G}_2$. In variant the expensive "hash-to-point" hash function maps into the group $\mathbb{G}_1$ but on the other hand we all exponentiations have to be carried out in $\mathbb{G}_2$ and furthermore the ciphertext lies in $\mathbb{G}_2$.

Our Scheme. We consider variants two and three of our IBE scheme from Table 2. Since we consider full IBE schemes ciphertexts consist of the IB-KEM ciphertext plus a summetric one-time encryption and a MAC. More precisely, the ciphertext space of our IBE scheme is $\mathbb{G}_a \times \mathbb{G}_b \times \{0,1\}^k \times \{0,1\}^m$, where the $\{0,1\}^k$ stands for the tag of the MAC (k bits are sufficient to guarantee security of k bits).

We estimate the cost of encryption and decryption using the timings for each atomic primitive (exponentiations/hashes in $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ and pairings) calculated in [24], where we used the timings for the "pairing friendly curves" and the Tate pairing. Here we counted one hash-into-curve operation used in the Boneh/Franklin scheme (the random oracle H_2) as one co-factor exponentiation [24]. For completeness all used timing data for the atomic primitives is given in Table 5 of Appendix A. The comparison is done with respect to the different curves A-H considered in [24], the names correspond the ones given therein. Important parameters for the curves are the estimated bits of security they provide, the embedding degree $\alpha = 6, 12, 24$, and the field size of the underlying finite field. We assume that one element in $\mathbb{G}_1$ can be represented using $\log_2 p$ bits. We furthermore assume that one element in $\mathbb{G}_2$ needs a factor of α as much space to represent as one element in $\mathbb{G}_1$, i.e. $\alpha \log_2 p$ bits.

Comparison. The extensive comparison matrix for the different curves A-H is given in Table 4. We conclude that efficiency of our scheme is comparable to the one from Boneh and Franklin — ciphertext sizes are more or less the same and encryption is a factor of 3 to 10 faster (depending on the chosen security parameter), whereas decryption of our scheme is about 1.5 to 3 times slower (depending on the variant). One disadvantage of our scheme seems to be the relatively large public-key ($n + 3$ group elements for n bit identities). We stress that with the techniques from Section 6.1 the public-key size can easily be shrunk to n/l group elements with losing only l bits of security.

The IBE scheme from Sakai and Kasahara [39]. We remark that in the random oracle model there also exists a more efficient IBE scheme that was recently proved secure by Chen and Cheng [15], and further analyzed and implemented by Chen et al. [16]. Its encryption speed it roughly 1.5 times faster than ours (and therefore 6 to 30 times faster than the one from Boneh/Franklin), and decryption speed is 2 to 3 times as fast (and therefore comparable to the one from Boneh/Franklin). Therefore it outperforms our IBE construction as well as the Boneh/Franklin IBE scheme. The drawback is, however, that its security relies on a seemingly much stronger assumption, the q_{hash}-BDDHI assump-

```
$\mathsf{Setup}(1^k)$
    $u, \alpha \xleftarrow{\$} \mathbb{G}_1^* \ ; \ z \leftarrow \hat{e}(\alpha, g_2) \in \mathbb{G}_T$
    $\mathsf{H} \xleftarrow{\$} \mathsf{HGen}(\mathbb{G}_1)$ //$\mathsf{H} = (h_0, \ldots, h_{10}) \in \mathbb{G}_1^{11}$
    $mpk \leftarrow (\mathsf{H}, u, z) \in \mathbb{G}_1^{12} \times \mathbb{G}_T \ ; \ msk \leftarrow \alpha \in \mathbb{G}_1$
    Return $(mpk, msk)$

$\mathsf{Extract}(msk, id)$
    $s \xleftarrow{\$} \mathbb{Z}_p$
    $sk[id] \leftarrow (\alpha \cdot \mathsf{H}(id)^s, g_2^s, u^s) \in \mathbb{G}_1 \times \mathbb{G}_2 \times \mathbb{G}_1$
    Return $sk[id]$

$\mathsf{Encaps}(mpk, id)$
    $r \xleftarrow{\$} \mathbb{Z}_p^*$
    $c_1 \leftarrow g_2^r \in \mathbb{G}_2 \ ; \ t \leftarrow \mathsf{TCR}(c_1)$
    $c_2 \leftarrow (\mathsf{H}(id) \cdot u^t)^r \in \mathbb{G}_1$
    $K \leftarrow z^r \in \mathbb{G}_T$
    $C \leftarrow (c_1, c_2) \in \mathbb{G}_1^2$
    Return $(C, K)$

$\mathsf{Decaps}(mpk, id, sk[id], C)$
    Parse $C$ as $(c_1, c_2)$
    Parse $sk[id]$ as $(d_1, d_2, d_3)$
    $t \leftarrow \mathsf{TCR}(c_1)$
    $v \xleftarrow{\$} \mathbb{Z}_p^*$
    Return $K \leftarrow \dfrac{\hat{e}(d_1 \cdot d_3^t \cdot (\mathsf{H}(id)u^t)^v, c_1)}{\hat{e}(c_2, g_2^v \cdot d_2)}$
```

Figure 2: A concrete instantiation of Variant 3 on curves with 80 bits security and recommended $l = 16$. We use an asymmetric pairing where $\mathbb{G}_1, \mathbb{G}_2$, and $\mathbb{G}_T$ are chosen according to the parameters of curve A from [24].

tion (as defined in Appendix C), where $q_{\text{hash}} \approx 2^{60}$ is the number of total random oracle queries an adversary can do in attacking the scheme.[5] In contrast our scheme can be proved secure under the mBDDH assumption which is according to Lemma 3.1 not stronger than the 2-BDDHI assumption. Due to the recently discovered security shortcomings of the q_{hash}-BDDHI assumption for large values of q_{hash} [17] known security guarantees of the Sakai/Kasahara IBE scheme should be taken with care until further research has been done in understanding the q_{hash}-BDDHI assumption.

7.4 A concrete instantiation of Variant 3

We conclude out paper by presenting details of a concrete instantiation of Variant 3 from Table 2. Let $\mathsf{TCR} : \mathbb{G} \to \mathbb{Z}_p$ be a target collision-resistant hash function, and let $\mathsf{CR} : \{0,1\}^* \to \{0,1\}^{80}$. All hash functions may be implemented in practise using a suitable variant of SHA-1. Let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ be an asymmetric pairing where $\mathbb{G}_1, \mathbb{G}_2$, and $\mathbb{G}_T$ are chosen according to the parameters of curve A in [24], and let g_2 be a fixed generator of G_2. Waters's hash function is defined as $\mathsf{H}(id) = h_0 \prod_{i=1}^{10} h_i^{id'_i} \in \mathbb{G}_1$, where $id' = (id'_1, \ldots, id'_{10}) \in (\{0,1\}^{16})^{10}$ and $id' = \mathsf{CR}(id)$ is the output of the collision resistant hash function CR (c.f. Section 6.1). All the above information is considered as public system parameters. Our IB-KEM with identity space $\mathsf{IDSp} = \{0,1\}^*$ and key space $\mathsf{KeySp} = \mathbb{Z}_p$ is depicted in Figure 2.

ACKNOWLEDGMENT. We thank Alex Dent, Javier Herranz, Dennis Hofheinz, John Malone-Lee, and Nigel Smart for their comments and suggestions.

References

[1] P. S. L. M. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order. In *Selected Areas in Cryptography – SAC'2005*, pages 319–331, 2006.

[2] 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, Santa Barbara, CA, USA, August 23–27, 1998. Springer-Verlag, Berlin, Germany.

[5] Bellare and Rogaway suggest to use $q_{\text{hash}} = 2^{60}$ for exact security reductions [4].

[3] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *ACM CCS 93*, pages 62–73, Fairfax, Virginia, USA, November 3–5, 1993. ACM Press.

[4] Mihir Bellare and Phillip Rogaway. The exact security of digital signatures: How to sign with RSA and Rabin. In Ueli M. Maurer, editor, *EUROCRYPT'96*, volume 1070 of *LNCS*, Saragossa, Spain, May 12–16, 1996. Springer-Verlag, Berlin, Germany.

[5] K. Bentahar, P. Farshim, J. Malone-Lee, and N.P. Smart. Generic constructions of identity-based and certificateless KEMs. Cryptology ePrint Archive, Report 2005/058, 2005. `http://eprint.iacr.org/`.

[6] Dan Boneh and Xavier Boyen. Efficient selective-id secure identity based encryption without random oracles. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 223–238, Interlaken, Switzerland, May 2–6, 2004. Springer-Verlag, Berlin, Germany.

[7] 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, Interlaken, Switzerland, May 2–6, 2004. Springer-Verlag, Berlin, Germany.

[8] Dan Boneh, Xavier Boyen, and Eu-Jin Goh. Hierarchical identity based encryption with constant size ciphertext. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 440–456, Aarhus, Denmark, May 22–26, 2005. Springer-Verlag, Berlin, Germany.

[9] Dan Boneh and Matthew K. Franklin. Identity based encryption from the Weil pairing. *SIAM Journal on Computing*, 32(3):586–615, 2003.

[10] Dan Boneh and Jonathan Katz. Improved efficiency for CCA-secure cryptosystems built using identity-based encryption. In Alfred Menezes, editor, *CT-RSA 2005*, volume 3376 of *LNCS*, pages 87–103, San Francisco, CA, USA, February 14–18, 2005. Springer-Verlag, Berlin, Germany.

[11] Xavier Boyen, Qixiang Mei, and Brent Waters. Direct chosen ciphertext security from identity-based techniques. In *ACM Conference on Computer and Communications Security—CCS 2005*, pages 320–329. New-York: ACM Press, 2005.

[12] Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited. In *30th ACM STOC*, pages 209–218, Dallas, Texas, USA, May 23–26, 1998. ACM Press.

[13] Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-ciphertext security from identity-based encryption. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 207–222, Interlaken, Switzerland, May 2–6, 2004. Springer-Verlag, Berlin, Germany.

[14] Sanjit Chatterjee and Palash Sarkar. Trading time for space: Towards an efficient ibe scheme with short(er) public parameters in the standard model. Proceedings of ICISC, to appear, 2005.

[15] L. Chen and Z. Cheng. Security proof of sakai-kasahara's identity-based encryption scheme. In *Proceedings of Cryptography and Coding 2005*, volume 2796 of *LNCS*, pages 442–459. Berlin: Springer-Verlag, 2005.

[16] L. Chen, Z. Cheng, J. Malone-Lee, and N.P. Smart. An efficient ID-KEM based on the sakai-kasahara key construction. Cryptology ePrint Archive, Report 2005/224, 2005. `http://eprint.iacr.org/`.

[17] J. H. Cheon. Security analysis of the strong diffie-hellman problem. In *EUROCRYPT 2006*, volume ???? of *LNCS*, pages ???–??? Berlin: Springer-Verlag, 2006.

[18] Clifford Cocks. An identity based encryption scheme based on quadratic residues. In Bahram Honary, editor, *Cryptography and Coding, 8th IMA International Conference*, volume 2260 of *LNCS*, pages 360–363, Cirencester, UK, December 17–19, 2001. Springer-Verlag, Berlin, Germany.

[19] Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In Hugo Krawczyk, editor, *CRYPTO'98*, volume 1462 of *LNCS*, pages 13–25, Santa Barbara, CA, USA, August 23–27, 1998. Springer-Verlag, Berlin, Germany.

[20] Ronald Cramer and Victor Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. *SIAM Journal on Computing*, 33(1):167–226, 2003.

[21] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Michael J. Wiener, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 537–554, Santa Barbara, CA, USA, August 15–19, 1999. Springer-Verlag, Berlin, Germany.

[22] Craig Gentry and Alice Silverberg. Hierarchical ID-based cryptography. In Yuliang Zheng, editor, *ASIACRYPT 2002*, volume 2501 of *LNCS*, pages 548–566, Queenstown, New Zealand, December 1–5, 2002. Springer-Verlag, Berlin, Germany.

[23] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28:270–299, 1984.

[24] R. Granger, D. Page, and N. P. Smart. High security pairing-based cryptography revisited. Cryptology ePrint Archive, Report 2006/059, 2006. `http://eprint.iacr.org/`.

[25] Shai Halevi and Phillip Rogaway. A tweakable enciphering mode. In Dan Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 482–499, Santa Barbara, CA, USA, August 17–21, 2003. Springer-Verlag, Berlin, Germany.

[26] Shai Halevi and Phillip Rogaway. A parallelizable enciphering mode. In Tatsuaki Okamoto, editor, *CT-RSA 2004*, volume 2964 of *LNCS*, pages 292–304, San Francisco, CA, USA, February 23–27, 2004. Springer-Verlag, Berlin, Germany.

[27] Jeremy Horwitz and Ben Lynn. Toward hierarchical identity-based encryption. In Lars R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 466–481, Amsterdam, The Netherlands, April 28 – May 2, 2002. Springer-Verlag, Berlin, Germany.

[28] IEEE P1363.3 Committee. IEEE 1363.3 / CfS — standard for identity-based cryptographic techniques using pairings. `http://grouper.ieee.org/groups/1363/index.html/`, February 2006. Call for submissions.

[29] Eike Kiltz and David Galindo. Direct chosen-ciphertext secure identity-based encryption without random oracles. Cryptology ePrint Archive, Report 2006/034, 2006. `http://eprint.iacr.org/`.

[30] Kaoru Kurosawa and Yvo Desmedt. A new paradigm of hybrid encryption scheme. In Matthew Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 426–442, Santa Barbara, CA, USA, August 15–19, 2004. Springer-Verlag, Berlin, Germany.

[31] B. Libert and J. Quisquater. Identity based encryption without redundancy. In *ACNS'05*, pages 285–300, 2005.

[32] Victor Miller. The Weil pairing, and its efficient calculation. *Journal of Cryptology*, 17(4), 2004.

[33] David Naccache. Secure and *practical* identity-based encryption. Cryptology ePrint Archive, Report 2005/369, 2005. `http://eprint.iacr.org/`.

[34] Moni Naor and Moti Yung. Universal one-way hash functions and their cryptographic applications. In *21st ACM STOC*, pages 33–43, Seattle, Washington, USA, May 15–17, 1989. ACM Press.

[35] Tatsuaki Okamoto. Efficient blind and partially blind signatures without random oracles. In Shai Halevi and Tal Rabin, editors, *TCC 2006*, LNCS, pages ???–???, New York, USA, February 5–7, 2006. Springer-Verlag, Berlin, Germany.

[36] D. Page, N.P. Smart, and F. Vercauteren. A comparison of MNT curves and supersingular curves. Cryptology ePrint Archive, Report 2004/165, 2004. `http://eprint.iacr.org/`.

[37] Duong Hieu Phan and David Pointcheval. Chosen-ciphertext security without redundancy. In Chi-Sung Laih, editor, *ASIACRYPT 2003*, volume 2894 of *LNCS*, pages 1–18, Taipei, Taiwan, November 30 – December 4, 2003. Springer-Verlag, Berlin, Germany.

[38] John Rompel. One-way functions are necessary and sufficient for secure signatures. In *22nd ACM STOC*, pages 387–394, Baltimore, Maryland, USA, May 14–16, 1990. ACM Press.

[39] R. Sakai and M. Kasahara. ID based cryptosystems with pairing on elliptic curve. Cryptology ePrint Archive, Report 2003/054, 2003. `http://eprint.iacr.org/`.

[40] Secure hash standard. National Institute of Standards and Technology, NIST FIPS PUB 180-1, U.S. Department of Commerce, April 1995.

[41] Adi Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and David Chaum, editors, *CRYPTO'84*, volume 196 of *LNCS*, pages 47–53, Santa Barbara, CA, USA, August 19–23, 1985. Springer-Verlag, Berlin, Germany.

[42] Victor Shoup. OAEP reconsidered. In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 239–259, Santa Barbara, CA, USA, August 19–23, 2001. Springer-Verlag, Berlin, Germany.

[43] Brent R. Waters. Efficient identity-based encryption without random oracles. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 114–127, Aarhus, Denmark, May 22–26, 2005. Springer-Verlag, Berlin, Germany.

A Timing data from [24].

The timing data used in our comparison in Section 7.3 is given in Table 5.

B Proof of Theorem 4.1

In this section we provide a game-based proof of Theorem 4.1. In fact in our proof some games could be absorbed nearly verbatim from [29], i.e. Games 1-4 are the nearyl same as Games 1-4 in [29]. The rest of the games are similar but due to the short ciphertexts and the different security assumption in our construction important and non-trivial changes had to be made to the respective games.

We will make use of the following simple "Difference Lemma" [42].

k	Curve $(\log_2 p, \alpha)$	exp $\mathbb{G}_1$	hash $\mathbb{G}_1$	exp $\mathbb{G}_2$	hash $\mathbb{G}_2$	exp $\mathbb{G}_T$	pairing	$\lvert\mathbb{G}_1\rvert$	$\lvert\mathbb{G}_2\rvert(\lvert G_T\rvert)$
80	A (160,6)	0.9	0	4.8	9.4	0.8	5.4	160	480
128	B (512,6)	14	14	69	330	11	101	512	1536
128	C (256,12)	3.6	0	50	243	5	63	256	1536
192	D (1365,6)	140	361	700	6419	120	1291	1365	4095
192	E (683,12)	36	28	494	4608	49	780	683	4098
256	F (2560,6)	644	2493	3223	42714	552	7345	2560	7680
256	G (1280,12)	163	241	2252	30377	217	4192	1280	7680
256	H (640,24)	42	10	1382	18480	115	2781	640	7680

Table 5: Timings in terms of estimated 32 bit multiplications needed to perform atomic primitives (scaled by 10^5) and representation of group elements in bits. Hashing into the groups $\mathbb{G}_1$ and $\mathbb{G}_2$ is dominated by a cofactor exponentiation which in case of hashing into $\mathbb{G}_1$ for curves A and C (nearly) for free due to the small cofactor. All data is taken from Section 5 of [24].

Lemma B.1 Let X_1,X_2, B be events defined in some probability distribution, and suppose that $X_1 \wedge \neg B \Leftrightarrow X_2 \wedge \neg B$. Then $|\Pr[X_1] - \Pr[X_2]| \leq \Pr[B]$.

We assume modified BDDH is hard, i.e. for any adversary $\mathcal{B}$ running for polynomial time $\mathbf{Time}_{\mathcal{B}}(k)$ we have $\mathbf{Adv}^{\text{mbddh}}_{\mathcal{G},\mathcal{B}}(k) = \epsilon(k)$, for a non-negligible function $\epsilon = \epsilon(k)$. We will show that for any adversary $\mathcal{A}$ against the chosen-ciphertext security of the IBE scheme running for time

$$\mathbf{Time}_{\mathcal{A}}(k) = \mathbf{Time}_{\mathcal{B}}(k) - \Omega(\epsilon^{-2} \cdot \ln(\epsilon^{-1}) + q)$$

and making a maximum of $q = q(k)$ key-derivation/decapsulation queries, we have

$$\mathbf{Adv}^{\text{cca}}_{\mathcal{IBKEM},\mathcal{A}}(k) \quad = \quad \mathcal{O}(nq \cdot (\epsilon + q/p) + \mathbf{Adv}^{\text{hash-tcr}}_{\mathsf{TCR},\mathcal{H}}(k)) \ .$$

Game 0. Fix an efficient adversary $\mathcal{A}$. We now define a game, Game 0, an interactive game between adversary $\mathcal{A}$ and a simulator. Game 0 is simply the same game as the IBE security experiment of Section 2.2 in which the simulator provides adversary $\mathcal{A}$'s environment. While describing the experiment we wll make a couple of conventions on how the simulator chooses the values appearing in its simulation. These conventions will be purely conceptual and, compared to the original experiment, do not change the distribution of any value appearing during the experiment. We will also make a couple of definitions of values appearing during the experiments.

We assume that in the beginning the simulator chooses some values a, b, and c, uniformly distributed from $\mathbb{Z}_p$. The whole simulation will depend on these values (i.e., the key generation will depend on a, b, where the challenge ciphertext will depend on c). In sequel games the simulator will "forget" the values a, b, and c and instead only use the values g^a, g^b, g^{b^2}, and g^c.

Key Generation. Initially the simulator runs the IBE key generation algorithm $\mathsf{Setup}(1^k)$ and obtains the public key $mpk = (u, z, \mathsf{H})$ and secret key $msk = \alpha$. We make the convention that the keys are generated as

$$u \xleftarrow{\$} g^b \ ; \qquad z \leftarrow \hat{e}(g^a, g^b) \ ; \qquad \mathsf{H} \xleftarrow{\$} \mathsf{HGen}(\mathbb{G}) \tag{1}$$

depending on the element g^a, g^b chosen by the simulator in advance. Note that the way the value $z = \hat{e}(g^a, g^b) = \hat{e}(g, g^{ab})$ from the public key is generated implies $\alpha = g^{ab} = u^a$. Note that α can be computed by the simulator since a is still known in this game. The public key is given to the adversary to start its `find` phase.

Find Phase. During its execution adversary $\mathcal{A}$ makes a number of key derivation and decapsulation requests. If the adversary makes a key derivation query $\mathsf{IBKeyDer}(id)$ then (using its secret key α)

the simulator computes the secret key $sk[id]$ and returns it to the adversary. If the adversary makes a decapsulation query $\textsc{Decaps}(id, C)$ the simulator (using α) decapsulates the ciphertext and returns the session key to the adversary.

Eventually, the adversary returns a target identity id^*. The simulator chosen a random key K_0^* and run the encapsulation algorithm to create a key K_1^* together with the the challenge ciphertext $C^* = (c_1^*, c_2^*)$. We make the convention that the challenge ciphertext $C^* = (c_1^*, c_2^*)$ is computed as

$$c_1^* \leftarrow g^c, \quad t^* \leftarrow \mathsf{TCR}(g^c), \quad c_2^* \leftarrow \mathsf{H}(id^*)^c u^{ct^*}, \tag{2}$$

depending on the random value c chosen by the simulator in advance, and the key $K_1^* = z^c$. Then the simulator chooses a random bit γ and the challenge ciphertext C^* together with the key $K^* = K_\gamma^*$ is returned to the adversary.

Guess Phase. The adversary continues to make its oracle queries, subsequent key derivation requests must be different from the target identity id^* and decapsulation requests must be different from (id^*, C^*). Finally, adversary $\mathcal{A}$ returns a bit $\gamma' \in \{0, 1\}$. If $\gamma \neq \gamma'$ the simulator returns $\beta' = 0$, else it returns $\beta' = 1$. This completes the description of the simulator. Note that the simulator behaves exactly as in the original IBE security experiment.

Now a few important definitions are in place. During its execution $\mathcal{A}$ may query the key derivation oracle for some identity id or the decapsulation oracle for the identity/ciphertext pair (id, C). We collect all those identities used to make queries to the key derivation and decapsulation oracle in the set $\widetilde{ID}$. Note that $\widetilde{ID}$ may contain the target identity id^* or one identity more than once. Let ID be the subset of queried identities obtained by removing from $\widetilde{ID}$ all multiples and the target identity. We write $ID = \{id^{(1)}, \ldots, id^{(q_0)}\}$ (without any particular order) for some $q_0 \leq q$ such that $id^{(i)} \neq id^{(j)}$ for each $1 \leq i \neq j \leq q_0$ and $id^* \notin ID$. Furthermore, we define $ID^* = ID \cup \{id^*\} = \{id^{(1)}, \ldots, id^{(q_0)}, id^*\}$.

The proof of the theorem is obtained by considering subsequent games, Game 1, Game 2, ..., These games will be quite similar to Game 0. In every game the simulators' output bit β' will be well-defined. For each i we define the event

$$X_i : \text{The simulator outputs } \beta' = 1 \text{ in Game } i.$$

Then, since in Game 0 the simulator exactly plays the IBE security experiment with adversary $\mathcal{A}$, we have

$$|\Pr[X_0] - 1/2| = \mathbf{Adv}^{\mathrm{cca}}_{\mathcal{IBKEM},\mathcal{A}} \ .$$

Game 1. (Eliminate hash collisions) Note that the values $c_1^* = g^c$ and $t^* = \mathsf{TCR}(g^c)$ from the challenge ciphertext Equation (2) are completely independent of the view of adversary $\mathcal{A}$ until $\mathcal{A}$'s guess phase (since c is simply not touched by the simulator before generating the challenge ciphertext). Therefore we may assume that the value c_1^* and t^* are already generated by the simulator before the key generation.

In this game the simulator changes its answers to all decapsulation queries $\textsc{Decaps}(id, C)$ made by $\mathcal{A}$ as follows: Let $C = (c_1, c_2)$ and $t = \mathsf{TCR}(c_1)$. If $t = t^*$ and $c_1 \neq c_1^*$, the simulator aborts. Otherwise it continues as in the last game. Let HashAbort be the event that this new abortion rule applies. Until HashAbort happens Game 0 and Game 1 are identical. Therefore by Lemma B.1 we have

$$|\Pr[X_1] - \Pr[X_0]| \leq \Pr[\textsc{HashAbort}] \ .$$

Furthermore,

$$\Pr[\textsc{HashAbort}] \leq \mathbf{Adv}^{\text{hash-tcr}}_{\mathsf{TCR},\mathcal{H}}(k) \ ,$$

i.e. there exists an adversary $\mathcal{H}$ against the target collision resistence of TCR (note that $c_1^* = g^c$ is a random element coming from outside $\mathcal{H}$'s view) running in time $\mathbf{Time}_{\mathcal{H}}(k) = \mathbf{Time}_{\mathcal{A}}(k) + \mathcal{O}(1)$ that succeeds with probability at least $\Pr[\textsc{HashAbort}]$.

Game 2. (Change of the hash keys) This is the same as Game 1 except that the simulator changes the generation of the hash keys $h = (h_0, h_1, \ldots, h_n)$ as follows.

Set $m = 2q$ (the choice of m will become clear later). Instead of generating the hash keys with the hash key-generation algorithm $\mathsf{HGen}(\mathbb{G})$ as in the last game the simulator chooses

$$\begin{aligned} x_0, x_1, \ldots, x_n &\overset{\$}{\leftarrow} \{0, \ldots, p-1\} \\ y_0', y_1, \ldots, y_n &\overset{\$}{\leftarrow} \{0, \ldots, m-1\} \\ k &\overset{\$}{\leftarrow} \{0, \ldots, n\} \qquad (3) \\ \text{and sets} & \\ y_0 &\leftarrow p - km + y_0' \;. \end{aligned}$$

The public keys $h = (h_0, \ldots, h_n)$ of the hash function H are then defined as $h_0 = (g^a)^{y_0} \cdot (g^b)^{-t^*} \cdot g^{x_0}$ and $h_i = g^{x_i}(g^a)^{y_i}$, for $1 \le i \le n$. The public hash function is $\mathsf{H}(id) = h_0 \prod_{i=1}^n h_i^{id_i}$. From the simulator's point of view, the hash function evaluated in identity $id \in \{0,1\}^n$ is

$$\mathsf{H}(id) = g^{x(id) + y(id)a - t^* b}, \qquad (4)$$

with $x(id) = x_0 + \sum_{i=1}^n id_i x_i$ and $y(id) = y_0 + \sum_{i=1}^n id_i y_i$ only known to the simulator. On the other hand note that this does not change the distribution of the hash keys $h = (h_0, h_1, \ldots, h_n)$. Therefore we have

$$\Pr[X_1] = \Pr[X_2] \;.$$

Game 3. (Abort at the end of the game) Fix all the random variables adversary $\mathcal{A}$ gets to see during its execution, including its random coin tosses: fix *mpk*, the challenge bit γ, and the randomness used in answering the key derivation and decapsulation queries. Now the adversary can be seen as a deterministic algorithm, in particular the set of all queried (distinct) identities $ID^* = \{id^{(1)}, \ldots, id^{(q_0)}, id^*\}$ can be seen as fixed. By $view_{\mathcal{A}}$ we denote all these fixed variables.

Define $\mathbf{Y} = (y_0', y_1, \ldots, y_n, k)$, where the random variables $(y_0', y_1, \ldots, y_n, k)$ are distributed as in Equation (3). It is clear that once $view_{\mathcal{A}}$ is fixed, the random variable $\mathbf{Y}$ still has its original distribution. Define the event

$$\textsc{ForcedAbort} : \bigvee_{i=1}^{q_0} \left(y(id^{(i)}) = 0 \bmod p \right) \vee y(id^*) \neq 0 \bmod p \;.$$

We call this abort *forced* since in sequel games the simulator is modified such that it always *has to* abort once this event happens. For fixed $view_{\mathcal{A}}$ we define

$$\eta := \Pr_{\mathbf{Y}}[\neg\textsc{ForcedAbort}] \qquad (5)$$

and let λ be a lower bound on η (that holds for every $view_{\mathcal{A}}$). The following lemma provides a lower bound on η.

Lemma B.2 For each possible choice of identities $ID^* = \{id^{(1)}, \ldots, id^{(q_0)}, id^*\}$ we have $\eta \ge \lambda = \frac{1}{4(n+1)q}$.

The proof of the lemma is given in [29].

Compared to Game 2 we will make two modifications to the simulator in Game 3. The simulation is exactly the same as in Game 2 until adversary $\mathcal{A}$ outputs his guess bit γ'. Since adversary $\mathcal{A}$ already terminated we can assume $\mathit{view}_{\mathcal{A}}$ to be fixed from now on.

First modification: add forced abort. After adversary $\mathcal{A}$ outputs his guess bit γ', the simulator checks if the event ForcedAbort occurs. If yes, it aborts the game and returns a random bit as its output bit β'. If not the simulation is continued as before.

Let's first make an unsuccessful attempt to relate the two events X_3 and X_2. Clearly we have $\Pr[X_3] = \Pr[X_2 \wedge \neg\textsc{ForcedAbort}] + 1/2 \cdot \Pr[\textsc{ForcedAbort}]$. Now we would like to continue with $\Pr[X_2 \wedge \neg\textsc{ForcedAbort}] \geq \Pr[X_2] \cdot \Pr[\neg\textsc{ForcedAbort}]$. However, this is not correct since the simulator may aborts with a probability that is a function in the choices of the identities $\mathit{ID}^* = \{\mathit{id}^{(1)}, \ldots, \mathit{id}^{(q_0)}, \mathit{id}^*\}$ queried by adversary $\mathcal{A}$ and hence the two events X_2 and $\neg$ForcedAbort cannot be considered as independent.

To get rid of this unwanted dependence the simulator adds some *artificial abort* such that it always aborts with probability nearly λ (recall that λ was is upper bound on the abortion probability), independent of the choices of the identities $\mathit{ID}^* = \{\mathit{id}^{(1)}, \ldots, \mathit{id}^{(q_0)}, \mathit{id}^*\}$. This way it will be possible to decorrelate the event X_2 with the abortion.

Second modification: add artificial abort. After the simulator has checked for the event ForcedAbort (and decided not to abort), it continues as follows: First it samples (using sufficiently many samples) an estimate η' of the probability η (over $\mathbf{Y}$) that the ForcedAbort happens (cf. Eqn. (5)).[6] We want to stress that $\mathit{view}_{\mathcal{A}}$ is fixed at this point so sampling does not involve running adversary $\mathcal{A}$ again. This estimate η' is a function in $\mathit{id}^{(1)}, \ldots, \mathit{id}^{(q_0)}, \mathit{id}^*$.
Depending on the estimate η' the simulator distinguishes two cases:
Case $\eta' \leq \lambda$: the simulator continues as before.
Case $\eta' > \lambda$: With probability $1 - \lambda/\eta'$ the simulator aborts and outputs a random bit β'. With probability λ/η' the simulator does not abort and continues as before.
This concludes the description of Game 3.

Lemma B.3 *Let $0 < \rho \leq 1$ be a function in k. If the simulator takes $\mathcal{O}(\rho^{-2}\ln(\rho^{-1}) \cdot \lambda^{-1}\ln(\lambda^{-1}))$ samples when computing the estimate η', then*

$$\left|\Pr[X_2] - \frac{1}{2} - \frac{\Pr[X_3] - 1/2}{\lambda}\right| \leq \frac{\rho}{2} .$$

The parameter ρ will be determined at the end of the proof.

Game 4. (Forced abort during the game I) Compared to the last game we make the following changes to the simulator: When identity $\mathit{id} \in \mathit{ID}$ is queried to the key derivation oracle, the simulator immediately aborts if $y(\mathit{id}) = 0 \bmod p$. When receiving the challenge identity id^*, the simulator immediately aborts if $y(\mathit{id}^*) \neq 0 \bmod p$. On abort the simulator returns a random bit β'. The artificial abort at the end of the simulation is the same as in the last game.

Clearly, this modification does not affect the adversary if there is no forced abort. In case there is a new forced abort the simulator outputs a random bit β' as in Game 3. Therefore we have

$$\Pr[X_4] = \Pr[X_3] .$$

Game 5. (Change key derivation oracle) The simulator changes its answers to all key derivation queries $\mathsf{IBKeyDer}(\mathit{id})$ made by the adversary $\mathcal{A}$ as follows: By Eqn. (4) we have $\mathsf{H}(\mathit{id}) =$

[6] Unfortunately, there seems not to be an efficient way to compute the exact value η. If there was one we could greatly simplify our analysis.

$g^{x(id)+y(id)a-t^*b}$, for some values $x(id)$ and $y(id)$ known to the simulator.
Case $y(id) = 0 \bmod p$: The simulator aborts (as in the last game).
Case $y(id) \neq 0 \bmod p$: The derived key $sk[id] = (d_1, d_2, d_3)$ is computed as follows:
For a random $r' \in \mathbb{Z}_p$, the simulator implicitly defines $r = -b/y(id) + r' \bmod p$ and computes

$$\begin{aligned}
d_1 &\leftarrow (g^a)^{y(id)r'} \cdot (g^b)^{-x(id)/y(id)-r't^*} \cdot (g^{b^2})^{t^*/y(id)} \cdot g^{x(id)r'} \\
d_2 &\leftarrow (g^b)^{-1/y(id)} \cdot g^{r'} \\
d_3 &\leftarrow (g^{b^2})^{-1/y(id)} \cdot (g^b)^{r'} .
\end{aligned}$$

Note that the randomness r is not known to the simulator and that the generation of the derived keys $sk[id]$ does not involve the knowledge of the secret key $\alpha = g^{ab}$ anymore.

Lemma B.4 $\Pr[X_4] = \Pr[X_5]$.

Proof: We have to verify that each derived key $sk[id] = (d_1, d_2, d_3)$ is identically distributed as in the last game. Let us abbreviate $x = x(id)$, and $y = y(id) \neq 0 \bmod p$. Clearly, if r' is uniform in $\mathbb{Z}_p$ then so is r. Then

$$\begin{aligned}
d_1 &= (g^a)^{yr'} \cdot (g^b)^{-x/y-r't^*} \cdot (g^{b^2})^{t^*/y} \cdot g^{xr'} \\
&= g^{ayr'-bx/y-br't^*+b^2t^*/y+xr'} \\
&= g^{ay(r+b/y)-bx/y-bt^*(r+b/y)^*+b^2t/y+x(r+b/y)} \\
&= g^{ayr+ab-bx/y-bt^*r-b^2t^*/y+b^2t^*/y+xr+xb/y} \\
&= g^{ayr+ab-bt^*r+xr} \\
&= \alpha \cdot (g^{ay-bt^*+x})^r \\
&= \alpha \cdot (\mathsf{H}(id))^r ,
\end{aligned}$$

and

$$\begin{aligned}
d_2 &= (g^b)^{-1/y} \cdot g^{r'} \\
&= g^{-b/y} g^{r-b/y} \\
&= g^r ,
\end{aligned}
\qquad\qquad
\begin{aligned}
d_3 &= (g^{b^2})^{-1/y} \cdot (g^b)^{r'} \\
&= u^{-b/y} u^{r-b/y} \\
&= u^r .
\end{aligned}$$

▮

Game 6. (Forced abort during the game II) Compared to the last game we make the following changes to the simulator: When the tuple (id, C) is queried to the decapsulation oracle for $id \in ID \cup \{id^*\}$ and $C = (c_1, c_2)$ the simulator computes $t = \mathsf{TCR}(c_1)$ and immediately aborts if $y(id) = 0 \bmod p$, C is consistent, and $t = t^*$. In case of abort the simulator returns a random bit β'.

Lemma B.5 $|\Pr[X_5] - \Pr[X_6]| \leq \frac{2q_2}{p}$, where q_2 is an upper bound on the number of decapsulation queries an adversary makes.

Proof: Clearly, this modification does not affect the adversary if there is no new forced abort. Note that a new forced abort implies $c_1 = c_1^*$ since otherwise by $t = t^*$ the simulator already aborted in the last game and found a collision in the hash function TCR. If there is a new forced abort we distinguish between two cases:

Case 1: the new forced abort happens in the `guess` stage. Recall that we call a ciphertext $C = (c_1, c_2)$ consistent if $(g, c_1, \mathsf{H}(id) \cdot u^t, c_2)$ is a Diffie-Hellman tuple (where $t = \mathsf{TCR}(c_1)$), i.e. if $(g, c_1, \mathsf{H}(id) \cdot u^t, c_2) = (g, g^r, \mathsf{H}(id) \cdot u^t, (\mathsf{H}(id) \cdot u^t)^r)$ for some value $r \in \mathbb{Z}_p$.

Note that the way the public-key is generated by Eqn. (4) and since $y(id) = 0$ and $t = t^*$, for any consistent ciphertext C we have

$$c_2 = (\mathsf{H}(id) \cdot u^t)^r = g^{r(x(id)+b(t-t)^*)} = (c_1^b)^{t-t^*} \cdot c_1^{x(id)} = c_1^{x(id)} \; . \tag{6}$$

If $id = id^*$ (i.e., if $\mathcal{A}$ queries the decapsulation oracle with the target identity) then Equation (6) implies $c_2 = c_1^{x(id)} = (c_1^*)^{x(id^*)} = c_2^*$. Consequently $C = C^*$ and so the simulator rejects as in the original IBE security experiment. If $id \neq id^*$ then, by definition, $id \in ID$ and the simulator outputs a random bit β' as in Game 5 where the abort was still done at the end of the experiment. Therefore, conditioned on case 1 we have $\Pr[X_5] = \Pr[X_6]$.

Case 2: the new forced abort happens in the `find` stage. Since in the find stage the adversary has no information (in a statistical sense) about c_1^* from the challenge ciphertext C^*, and the adversary makes at most q_2 decapsulation queries in its find stage, this implies

$$|\Pr[X_5] - \Pr[X_6]| \leq \frac{1}{p} + \frac{1}{p-1} + \ldots + \frac{1}{p-q_2+1} \leq \frac{q_2}{p-q_2} \leq \frac{2q_2}{p} \; ,$$

as claimed. ▌

Game 7. (Change the answers to the decapsulation queries.) The simulator changes its answers to all decapsulation queries $\textsc{Decaps}(id, C)$ made by $\mathcal{A}$ as follows: By Eqn. (4) we have $\mathsf{H}(id) = g^{x(id)+y(id)a-t^*b}$ for some values $x(id)$ and $y(id)$ known to the simulator.
Case $y(id) \neq 0 \bmod p$: the query is answered using the key derivation oracle.
Case $y(id) = 0 \bmod p$: the simulator simulates the decapsulation queries as follows: Let $C = (c_1, c_2, E)$ be the queried ciphertext and let $t = \mathsf{TCR}(c_1)$.

> If the ciphertext is not consistent then return a random session key K
> If $t = t^*$ then the simulator aborts (as in the last game)
> If $t \neq t^*$ then return $K \leftarrow \hat{e}(c_2/c_1^{x(id)}, g^a)^{(t-t^*)^{-1}}$

We claim that these changes do not affect the view of $\mathcal{A}$:

Lemma B.6 $\Pr[X_6] = \Pr[X_7]$.

Proof of Lemma B.6: Let $C = (c_1, c_2)$ be an arbitrary ciphertext submitted to the decapsulation oracle with respect to identity id. In case $y(id) \neq 0 \bmod p$ decapsulation will be done using the simulation of the key derivation oracle which we already showed to be correct so we may now assume $y(id) = 0 \bmod p$. Every inconsistent ciphertext leads to a random key K as in the original description of the scheme so in what follows we may also assume a consistent ciphertext.

We distinguish the following three cases: Case 1a: $t = t^*$ and $c_1 \neq c_1^*$. In this case the simulator has found a collision in the hash function TCR and aborts as in the last game.
Case 1b: $t = t^*$ and $c_1 = c_1^*$. In the case the simulator aborts as in forced abort introduced in the last game.

Case 2: $t \neq t^*$. Similar to Eqn. (6) consistency of C implies

$$c_2 = (\mathsf{H}(id) \cdot u^t)^r = g^{r(x(id)+b(t-t)^*)} = (c_1^b)^{t-t^*} \cdot c_1^{x(id)} \; ,$$

and we obtain

$$(c_2/c_1^{x(id)})^{(t-t^*)^{-1}} = ((c_1^b)^{t-t^*} \cdot c_1^{x(id)}/c_1^{x(id)})^{(t-t^*)^{-1}} = c_1^b \ . \tag{7}$$

In the original IBE decapsulation algorithm first the user secret key for identity id is computed as $sk[id] = (d_1, d_2, d_3) = (\alpha \cdot \mathsf{H}(id)^s, g^s, u^s)$ for random s, and then the session key K is reconstructed as

$$\begin{aligned} K = \hat{e}(c_1, d_1 \cdot d_3^t)/\hat{e}(c_2, d_2) &= \hat{e}(c_1, \alpha \cdot \mathsf{H}(id)^s \cdot (u^s)^t)/\hat{e}(c_2, g^s) \\ &= \hat{e}(c_1^b, g^a) \cdot \hat{e}(c_1, \mathsf{H}(id)^s \cdot (u^s)^t)/\hat{e}(c_2, g^s) \\ &\overset{(7)}{=} \hat{e}((c_2/c_1^{x(id)})^{(t-t^*)^{-1}}, g^a) \cdot (\hat{e}(c_1, \mathsf{H}(id) \cdot u^t)/\hat{e}(c_2, g))^s \\ &= \hat{e}(c_2/c_1^{x(id)}, g^a)^{(t-t^*)^{-1}} \cdot (\Delta(C))^s \ , \end{aligned}$$

with $\Delta(C) = \hat{e}(c_1, \mathsf{H}(id) \cdot u^t)/\hat{e}(c_2, g)$. Since $(\Delta(C))^s = 1$ if $\hat{e}(c_1, \mathsf{H}(id)u^t) = \hat{e}(g, c_2)$ and $(\Delta(C))^s$ is a random element in $\mathbb{G}_T$ otherwise, the decapsulated session key in the original scheme is distributed as in the simulation. ▌

Game 8. (Modify the challenge) After $\mathcal{A}$'s `find` stage the simulator inputs the target identity id^* from $\mathcal{A}$. The simulator modifies the computation of the challenge ciphertext C^* follows:
Case $y(id^*) \neq 0 \bmod p$: The simulator aborts (as in the last game).
Case $y(id^*) = 0 \bmod p$: The simulator chooses a random bit γ and creates the challenge ciphertext $C^* = (c_1^*, c_2^*)$ and key K_1^* as

$$c_1^* \leftarrow g^c, \quad c_2^* \leftarrow c_2^* \leftarrow (g^c)^{x(id^*)}, \quad K_1^* \leftarrow \hat{e}(g, g)^{abc} \ . \tag{8}$$

By virtue of Eqns. (4), (6), and since $\mathsf{TCR}(c_1^*) = t^*$ and $y(id^*) = 0 \bmod p$, C^* is a correctly distributed ciphertext of K_1^*. Clearly,

$$\Pr[X_9] = \Pr[X_8] \ .$$

Game 9. (Replace the Challenge) The simulator replaces the value K_1^* from the challenge C^* with a random element from $\mathbb{G}_T$. Since K_1^* is now completely independent of the challenge bit γ, we have

$$\Pr[X_{10}] = 1/2 \ .$$

Observe that Game 10 does not use the secret key anymore and that the whole simulation only depends on the values g^a, g^b, g^{b^2}, g^c (i.e., the simulator "forgot the values a, b, and c). Game 8 and Game 9 are equal unless adversary $\mathcal{A}$ can distinguish $\hat{e}(g, g)^{abc}$ (the value of K_1^* in Game 8) from a random element in $\mathbb{G}_T$ (the value of K_1^* in Game 9). Therefore we have

$$|\Pr[X_9] - \Pr[X_8]| \leq \mathbf{Adv}^{\mathrm{mbddh}}_{\mathcal{G},\mathcal{B}}(k),$$

for any adversary $\mathcal{B}$ against the hardness of mBDDH running in the same time as the simulator, i.e. $\mathbf{Time}_{\mathcal{B}} = \mathbf{Time}_{\mathcal{A}} + \mathcal{O}(\rho^{-2} \ln(\rho^{-1}) \cdot \lambda^{-1} \cdot \ln(\lambda^{-1}) + q)$.

Analysis. We collect the probabilities relating the different games as follows:

$$\begin{aligned}
\mathbf{Adv}^{\mathrm{cca}}_{\mathcal{IBKEM},\mathcal{A}} &= |\Pr[X_0] - \frac{1}{2}| \\
&\leq |\Pr[X_1] + \mathbf{Adv}^{\mathrm{hash\text{-}tcr}}_{\mathsf{TCR},\mathcal{H}}(k) - \frac{1}{2}| \\
&\leq |\Pr[X_2] - 1/2 + \mathbf{Adv}^{\mathrm{hash\text{-}tcr}}_{\mathsf{TCR},\mathcal{H}}(k)| \\
&\leq |\frac{\Pr[\,X_3\,] - \frac{1}{2}}{\lambda} + \frac{\rho}{2} + \mathbf{Adv}^{\mathrm{hash\text{-}tcr}}_{\mathsf{TCR},\mathcal{H}}(k)| \\
&\leq \frac{|\Pr[\,X_6\,] + \frac{2q_2}{p} - \frac{1}{2}|}{\lambda} + \frac{\rho}{2} + \mathbf{Adv}^{\mathrm{hash\text{-}tcr}}_{\mathsf{TCR},\mathcal{H}}(k) \\
&\leq \frac{|\Pr[\,X_9\,] + \frac{2q_2}{p} - \frac{1}{2}|}{\lambda} + \frac{\rho}{2} + \mathbf{Adv}^{\mathrm{hash\text{-}tcr}}_{\mathsf{TCR},\mathcal{H}}(k) \\
&\leq \frac{\mathbf{Adv}^{\mathrm{mbddh}}_{\mathcal{G},\mathcal{B}}(k) + \frac{2q_2}{p}}{\lambda} + \frac{\rho}{2} + \mathbf{Adv}^{\mathrm{hash\text{-}tcr}}_{\mathsf{TCR},\mathcal{H}}(k)\ .
\end{aligned}$$

Using $\lambda = \frac{1}{4(n+1)q}$ (by Lemma B.2) and defining $\rho = \min\{1, \frac{\mathbf{Adv}^{\mathrm{mbddh}}_{\mathcal{G},\mathcal{B}}(k)}{\lambda}\} \leq 1$ we conclude the proof with

$$\begin{aligned}
\mathbf{Adv}^{\mathrm{cca}}_{\mathcal{IBKEM},\mathcal{A}}(k) &\leq 6(n+1)q \cdot (\mathbf{Adv}^{\mathrm{mbddh}}_{\mathcal{G},\mathcal{B}}(k) + 2q_2/p) + \mathbf{Adv}^{\mathrm{hash\text{-}tcr}}_{\mathsf{TCR},\mathcal{H}}(k) \\
&= \mathcal{O}\Big(nq \cdot (\mathbf{Adv}^{\mathrm{mbddh}}_{\mathcal{G},\mathcal{B}}(k) + q/p) + \mathbf{Adv}^{\mathrm{hash\text{-}tcr}}_{\mathsf{TCR},\mathcal{H}}(k)\Big)\ ,
\end{aligned}$$

where q is an upper bound on all (derivation plus decapsulation) queries made by $\mathcal{A}$,

$$\begin{aligned}
\mathbf{Time}_{\mathcal{B}}(k) &= \mathbf{Time}_{\mathcal{A}}(k) + \mathcal{O}(\rho^{-2}\ln(\rho^{-1}) \cdot \lambda^{-1} \cdot \ln(\lambda^{-1}) + q) \\
&= \mathbf{Time}_{\mathcal{A}}(k) + \mathcal{O}(\epsilon^{-2}\ln(\epsilon^{-1}) + q)\ ,
\end{aligned}$$

where $\epsilon = \epsilon(k) = \mathbf{Adv}^{\mathrm{mbddh}}_{\mathcal{G},\mathcal{B}}(k)$, and

$$\mathbf{Time}_{\mathcal{H}}(k) \ = \ \mathbf{Time}_{\mathcal{A}}(k) + \mathcal{O}(1)\ .$$

C Relations between the Assumptions

C.1 The BDDH assumption

Let $\mathcal{PG}$ be the description of bilinear groups and let $g \in \mathbb{G}$ be a random element from group $\mathbb{G}$ of prime order p. Consider the following problem formalized by Boneh and Franklin [9]: Given $(g, g^a, g^b, g^c, W) \in \mathbb{G}^4 \times \mathbb{G}_2$ as input, output yes if $W = \hat{e}(g,g)^{abc}$ and no otherwise. The corresponding BDDH assumption can be formalized the same way as the modified BDDH assumption.

C.2 The q-BDDHI assumptions

Let $\mathcal{PG}$ as above and let $z \in \mathbb{G}$ be a random element from group $\mathbb{G}$. Let $q = q(k)$ be a function polynomial in the security parameter. Associated to q the following problem introduced by Boneh and Boyen [6]: Given $(h, h^a, h^{(a^2)}, \ldots, h^{(a^q)}, W) \in \mathbb{G}^{q+1} \times \mathbb{G}_2$ as input, output yes if $W = \hat{e}(h,h)^{1/a}$ and no otherwise.

```
$\mathsf{IBEkg}(1^k)$
    $\alpha \xleftarrow{\$} \mathbb{G}^*$ ; $z \leftarrow \hat{e}(g, \alpha)$
    $\mathsf{H} \xleftarrow{\$} \mathsf{HGen}(m)$
    $mpk \leftarrow (\mathsf{H}, z)$ ; $msk \leftarrow \alpha$
    Return $(mpk, msk)$

$\mathsf{IBEkeyder}(msk, id)$
    $s \xleftarrow{\$} \mathbb{Z}_p$
    $sk[id] \leftarrow (\alpha \cdot \mathsf{H}(id)^s, g^s)$
    Return $sk[id]$

$\mathsf{IBEenc}(mpk, id, M)$
    $r \xleftarrow{\$} \mathbb{Z}_p^*$ ; $c_1 \leftarrow g^r$ ; $c_2 \leftarrow \mathsf{H}(id)^r$
    $e \leftarrow M \cdot z^r$
    $C \leftarrow (c_1, c_2, e) \in \mathbb{G}^2 \times \mathbb{G}_T$
    Return $C$

$\mathsf{Decaps}(sk[id], C)$
    Parse $C$ as $(c_1, c_2, e)$
    Parse $sk[id]$ as $(d_1, d_2)$
    Return $M \leftarrow e \cdot \hat{e}(c_2, d_2)/\hat{e}(c_1, d_1)$
```

Figure 3: CPA-secure IBE from Waters.

C.3 Proof of Lemma 3.1

Proof: The implications BDDH $\leq$ mBDDH and 1-BDDHI $\leq$ 2-BDDHI $\leq$ 3-BDDHI $\leq \ldots$ are easy to show. To prove "modified BDDH assumption $\leq$ 2-BDDHI assumption", assume there exists a polynomial-time adversary $\mathcal{A}$ that breaks the modified BDDH assumption. We show that then there exists a polynomial-time adversary $\mathcal{B}$ with oracle access to $\mathcal{A}$ that breaks the 2-BDDHI assumption. Let (h, h^a, h^{a^2}, W) be an input instance of the 2-BDDHI problem given to $\mathcal{B}$. $\mathcal{B}$'s goal is to find out if $W = \hat{e}(h,h)^{1/a}$ or W is random. $\mathcal{B}$ picks two random values y_0, z_0 and defines its output bit as $\gamma := \gamma'$, where γ' is input from $\mathcal{A}$ as

$$\gamma' \leftarrow \mathcal{A}(h^{a^2}, h^a, h, h^{y_0}, h^{z_0}, W' = W^{y_0 z_0}).$$

We now show correctness. Defining $g := h^{a^2}$, $x = 1/a$, $y = y_0/a^2$, and $z = z_0/a^2$, we have $h^a = g^{1/a} = g^x$ and $h = g^{1/a^2} = g^{x^2}$. Consequently, $(h^{a^2}, h^a, h, h^{y_0}, h^{z_0}) = (g, g^x, g^{x^2}, g^y, g^z)$. If $W = \hat{e}(h,h)^{1/a}$, then

$$W' = W^{y_0 z_0} = \hat{e}(h,h)^{1/a \cdot y_0 \cdot z_0} = \hat{e}(g,g)^{1/a^5 \cdot y_0 z_0} = \hat{e}(g,g)^{1/a \cdot y_0/a^2 \cdot z_0/a^2} = \hat{e}(g,g)^{xyz}.$$

If W is a random element, so is W'. This proves the lemma. ▌

D Known IBE constructions

D.1 The IBE scheme from Waters [43]

Waters IBE scheme with identity space $\mathsf{IDSp} = \{0,1\}^n$ and message space $\mathsf{MsgSp} = \mathbb{G}_T$ is depicted in Figure 3.

D.2 The IBE scheme from Boneh/Franklin [9]

The Boneh/Franklin fullident IBE scheme with identity space $\mathsf{IDSp} = \{0,1\}^n$ and $\mathsf{MsgSp} = \{0,1\}^m$ is depicted in Figure 4. It needs four random oracles $\mathsf{H}_1 : \{0,1\}^n \rightarrow \mathbb{G}_2, \mathsf{H}_2 : \mathbb{G}_T \rightarrow \{0,1\}^{2k}, \mathsf{H}_3 : \{0,1\}^k \times \mathsf{MsgSp} \rightarrow \mathbb{Z}_p^*$, and $\mathsf{H}_4 : \{0,1\}^k \rightarrow \{0,1\}^m$.

```
$\mathsf{IBEkg}(1^k)$
    $\alpha \xleftarrow{\$} \mathbb{G}^*$
    Pick random oracles $\mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_3, \mathsf{H}_4$
    $mpk \leftarrow (\mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_3, \mathsf{H}_4)$ ; $msk \leftarrow \alpha$
    Return $(mpk, msk)$
```

```
$\mathsf{IBEkeyder}(msk, id)$
    $sk[id] \leftarrow \mathsf{H}_1(id)^\alpha \in \mathbb{G}_2$
    Return $sk[id]$
```

```
$\mathsf{IBEenc}(mpk, id, M)$
    $\sigma \xleftarrow{\$} \{0,1\}^k$ ; $r \leftarrow \mathsf{H}_3(\sigma, M)$
    $c_1 \leftarrow g^r$ ; $c_2 \leftarrow \sigma \oplus \mathsf{H}_2(\hat{e}(g, \mathsf{H}_1(id))^r)$
    $e \leftarrow \mathsf{H}_4(\sigma) \oplus M$
    $C \leftarrow (c_1, c_2, e) \in \mathbb{G} \times \{0,1\}^{2k} \times \{0,1\}^m$
    Return $C$
```

```
$\mathsf{IBEdec}(sk[id], C)$
    Parse $C$ as $(c_1, c_2, e)$
    $c_2 \leftarrow c_2 \oplus \mathsf{H}_2(\hat{e}(c_1, sk[id]))$
    $M \leftarrow e \oplus \mathsf{H}(\sigma)$
    $r \leftarrow \mathsf{H}_3(\sigma, M)$ ; if $g^r \neq c_1$ then reject
    Else return $M$
```

Figure 4: CCA-secure fullident IBE scheme from Boneh/Franklin.