CCA Secure IB-KEM from the Computational Bilinear Diffie-Hellman Assumption in the Standard Model

Yu Chen[1,2], Liqun Chen[3], and Zongyang Zhang[4,⋆]

[1] Institute of Information Engineering, Chinese Academy of Sciences
[2] State Key Laboratory of Information Security, Beijing, China
chenyu@is.iscas.ac.cn
[3] Hewlett-Packard Laboratories, Bristol, United Kingdom
liqun.chen@hp.com
[4] Department of Computer Science and Engineering
Shanghai Jiao Tong University, Shanghai, China
zongyang.zhang@gmail.com

Abstract. In this paper, we propose several selective-identity chosen-ciphertext attack secure identity based key encapsulation (IB-KEM) schemes that are provably secure under the computational bilinear Diffie-Hellman (CBDH) assumption in the standard model. Our schemes compare favorably to previous results in efficiency. With delicate modification, our schemes can be strengthened to be full-identity CCA secure easily.

Keywords: identity based encryption, standard model, CCA security, CBDH assumption

1 Introduction

1.1 Background

Security against adaptive chosen ciphertext attack (CCA security for short) is nowadays considered the commonly accepted security notion for public key encryption (PKE)/identity based encryption (IBE). One of the most important research direction in this field is to design CCA-secure PKE/IBE schemes based on weak security assumptions in the standard model.

Cramer and Shoup [CS98] proposed the first practical CCA-secure PKE scheme without random oracles. Their construction was later generalized to hash proof systems [CS02]. However, all its variants [KD04, BMW05, Kil06, Kil07, HK07, HK09] inherently rely on decisional assumption, e.g., the decisional Diffie-Hellman (DDH) assumption, the decisional bilinear Diffie-Hellman (DBDH) assumption or the decisional quadratic residuosity assumption. CCA security from computational assumptions was considered to be hard to obtain. Canetti, Halevi and Katz [CHK04] made the breakthrough in 2004. They proposed the first practical CCA-secure PKE scheme based on CBDH assumption. Later, Cash *et al.* [CKS08] presented a variant of Cramer-Shoup scheme [CS98] which is CCA-secure based on the strong twin CDH assumption, and in turn based on the standard CDH assumption. However, n group elements (where the value n is the bit-length of keys) have to be added into the ciphertext in order to prove CCA security. Hanaoka and Kurosawa [HK08] presented a CCA-secure PKE scheme enjoying the constant size ciphertext based on the CDH assumption from broadcast encryption. Hofheinz and Kitz [HK09] presented a construction assuming the hardness of factoring. Cramer, Hofheinz and Kitz [CHK10] refined the well-known Naor-Yung paradigm [NY90] and constructed practical CCA-secure PKE schemes based on hard search problems, which includes the CDH and RSA type assumptions. Wee [Wee10] gave more efficient and general transformations to CCA secure PKE schemes from extractable hash proof system, which again can be based on the hardness of CDH, RSA and factoring. Haralambiev, Jager, Kiltz and Shoup [HJKS10] then proposed a

⋆ Corresponding author

number of new PKE schemes that are provably secure under the CDH/CBDH assumption in the standard model, which improved efficiency of prior schemes from [CKS08, HK08].

For the time being, although there are several practical CCA-secure PKE schemes based on computational assumptions, CCA-secure IBE schemes based on weak assumptions are rare. This forms the main motivation of our work.

1.2 Our Contributions

In this paper we propose a number of new IB-KEM schemes that are CCA-secure under the CBDH assumption in the standard model. Our main idea is to extend the technique of constructing CCA-secure PKE schemes [HJKS10] to the IB-KEM version of Boneh-Boyen "commutative-blinding" IBE scheme (known as BB_1-IBE) [BB04]. We begin from a basic 1-bit IB-KEM, then extend it to n-bits IB-KEMs using different methods. As shown in Table 1 at the end of this section, our schemes improve efficiency of prior scheme [Gal10].

A 1-bit IB-KEM Scheme. We first construct a 1-bit IB-KEM scheme. We denote it by Scheme 0 and briefly describe it as follows.

$$\begin{array}{ll} \mathsf{Setup}: & mpk = (g, h, X = g^a, X', Y), msk = a \\ \mathsf{KeyGen}: & sk = (Y^a F(I)^s, g^s), \text{where } F(I) = X^I h \\ \mathsf{Encap}: & C = (g^r, (X^t X')^r, F(I)^r), \text{where } t = \mathsf{TCR}(g^r) \\ & K = f_{\mathrm{gl}}(e(X, Y)^r, R) \end{array}$$

Decryption only returns K if the ciphertext $C = (C_1, C_2, C_3)$ is consistent, i.e., $e(C_1, X^t X') = e(g, C_2) \wedge e(C_1, F(I)) = e(g, C_3)$. In all other cases it rejects and returns $\perp$. We defer the detailed construction and security proof to Section 3.

In what follows, we give a brief explanation of our strategy to achieve indistinguishability of ciphertext under selective-identity CCA attack (IND-sID-CCA) from two aspects, one is how to obtain selective-identity CCA security, and the other is how to reduce it to the CBDH assumption.

We first give the intuition behind the CCA security. From the attacker's view, the second part of the ciphertext $C_2 = (X^t X')^r$ prohibits an adversary from modifying a valid ciphertext in a meaningful way. From the challenger's view, the consistency of ciphertext is publicly verifiable, i.e., anyone could check the consistency of ciphertext with the help of bilinear map. Therefore any inconsistent ciphertext will be rejected. On the other hand, in the simulation all consistent ciphertexts can be classified into the following three types. Type-1 ciphertext is the one whose t value differs to t^* of the challenge ciphertext. Type-2 ciphertext is the one encrypted under an identity different from the challenge identity I^*. Type-3 ciphertext is exactly the challenge ciphertext. The reduction algorithm is able to decrypt all the consistent ciphertexts correctly by implementing dual all-but-one technique: set $X' := X^{-t^*} g^d$ to implement the all-but-one technique (with respect to $t \neq t^*$) to decrypt Type-1 ciphertexts ($t \neq t^*$); set $F(I) := X^{I-I^*} g^z$ to implement the all-but-one technique (with respect to $I \neq I^*$) to extract a private key for all identities but the challenge identity I^*, thus to be able to decrypt Type-2 ciphertexts ($I \neq I^*$). Type-3 ciphertext ($I = I^* \wedge t = t^*$) is not allowed to be queried according to the definition of selective-identity chosen ciphertext security model. To summarize, the reduction algorithm can handle all the decryption queries correctly.

We then give our basic idea about how to reduce the IND-sID-CCA security to the CBDH assumption. Note that the indistinguishable type security notion is essentially defined as a decisional problem. Considering the gap between decisional problems and computational problems, it would be difficult to directly reduce the IND-sID-CCA security to the CBDH assumption.

A natural approach is to find a stepping stone. More specifically, we first reduce the IND-sID-CCA security to some decisional assumption related to the CBDH assumption, then reduce the decisional assumption to the CBDH assumption. In this way the IND-sID-CCA security can be finally reduced to the CBDH assumption. We provide more details as follows. We select the Goldreich-Levin version decisional BDH (GL-DBDH) assumption [HJKS10] as the stepping stone, which states that there is no PPT algorithm that can distinguish the two distributions $\Delta_{\text{bdh}} = (g, A, B, C, K, R)$ and $\Delta_{\text{rand}} = (g, A, B, C, U, R)$. Here (g, A, B, C) are the inputs of a BDH problem, K is the output of a Goldreich-Levin hardcore predicate with $\text{bdh}(A, B, C)$ and randomness R as input while U is a bit sampled from $\{0, 1\}$ uniformly random. Suppose a reduction algorithm $\mathcal{B}$ is asked to solve the GL-DBDH problem. $\mathcal{B}$ simulates a real attack game of Scheme 0 by embedding A into X, embedding B into Y, and embedding C into one part of the challenge ciphertext. We demonstrate that if there exists an IND-sID-CCA adversary $\mathcal{A}$ that can break the CCA security of Scheme 0, then $\mathcal{B}$ can break the GL-DBDH assumption. The GL-DBDH assumption can be thus reduced to the CBDH assumption according to the Goldreich-Levin theorem. Therefore, the IND-sID-CCA security of Scheme 0 is finally reduced to the CBDH assumption.

We note that Scheme 0 bears a close resemblance to the IB-KEM scheme [KG06]. The key difference between the two schemes is the derivation of the symmetric key. In [KG06] the Encap algorithm directly uses a BDH seed as a symmetric key, while in Scheme 0 the Encap algorithm uses the Goldreich-Levin hardcore predicate to derive a 1-bit symmetric key from a BDH seed.

Note that the element $(X^t X')^r$ and $F(I)^r$ in the ciphertext share the same randomness r, thus it is possible to further shrink the public parameters size and the ciphertext size. By using a technique similar to [KV08], the ciphertext can be reduced to two group elements at the cost of adding one group element in the private key and resorting to a stronger assumption, named the modified CBDH assumption. We denote the resulting scheme by Scheme $0'$. The concrete construction and security proof are included in Appendix A.

A Scheme with constant size public parameters. To encapsulate a n-bits symmetric key, we can follow the standard multiple encapsulations method: perform the 1-bit IB-KEM n times using independent random coins. We denote the resulting scheme by Scheme 1 and describe it as follows.

$$
\begin{array}{ll}
\mathsf{Setup}: & mpk = (g, h, X = g^a, X', Y), msk = a \\
\mathsf{KeyGen}: & sk = (Y^a F(I)^s, g^s) \\
\mathsf{Encap}: & C = (C_1, \ldots, C_n), \text{where } C_i = (g^{r_i}, (X^t X')^{r_i}, F(I)^{r_i}) \\
& \text{with } t = \mathsf{TCR}(C_{i,1}, \ldots, C_{n,1}). \\
& K = (K_1, \ldots, K_n), \text{where } K_i = f_{\text{gl}}(e(X, Y)^{r_i}, R)
\end{array}
$$

We defer the detailed construction and security proof to Section 4.

A Scheme with constant size ciphertext. In contrast to the multiple encapsulations method used in Scheme 1, we may also adopt the randomness-reusing technique: include n group elements $(Y_1, \ldots, Y_n)$ into mpk (instead of a solo group element Y in previous schemes), then generate n BDH seeds using a single randomness r with respect to n different bases $e(X, Y_i)$. We denote the resulting scheme by Scheme 2 and describe it as follows.

$$
\begin{array}{ll}
\mathsf{Setup}: & mpk = (g, h, X = g^a, X', Y_1, \ldots, Y_n), msk = a \\
\mathsf{KeyGen}: & sk = (sk_i, \ldots, sk_n), \text{where } sk_i = (Y_i^a F(I)^{s_i}, g^{s_i}) \\
\mathsf{Encap}: & C = (g^r, (X^t X')^r, F(I)^r), \text{where } t = \mathsf{TCR}(g^r) \\
& K = (K_1, \ldots, K_n), \text{where } K_i = f_{\text{gl}}(e(X, Y_i)^r, R)
\end{array}
$$

We defer the detailed construction and security proof to Section 5.

Generalized Scheme 1. Scheme 1 enjoys the constant-size mpk but its ciphertext size is linear in n, while Scheme 2 enjoys the constant-size ciphertext but its mpk size is linear in n. It is interesting to know if there exists a trade-off between mpk size and ciphertext size. From the above two schemes, it is easy to see that when generating n pair-wise independent BDH seeds, the roles of Y_i and the randomness r_j are exchangeable. With this observation, we propose the following generalized scheme that offers a trade-off between mpk and ciphertext. We denote it by Scheme 3 and described it as follows. The detailed construction and security proof are deferred to Section 6.

$$
\begin{array}{ll}
\mathsf{Setup}: & mpk = (g, h, X = g^a, X', Y_1, \ldots, Y_{n_1}), msk = a \\
\mathsf{KeyGen}: & sk = (sk_i, \ldots, sk_{n_1}), \text{where } sk_i = (Y_i^a F(I)^{s_i}, g^{s_i}) \\
\mathsf{Encap}: & C = (C_1, \ldots, C_{n_2}), \text{where } C_i = (g^{r_i}, (X^t X')^{r_i}, F(I)^{r_i}) \\
& \text{with } t = \mathsf{TCR}(C_{i,1}, \ldots, C_{n_2,1}) \\
& K = (K_{i,j}) \text{ for } 1 \le i \le n_1, 1 \le j \le n_2, \text{ where } K_{i,j} = f_{\mathrm{gl}}(e(X, Y_i)^{r_j}, R)
\end{array}
$$

In the above generalized scheme, $(Y_1, \ldots, Y_{n_1})$ are n_1 independent elements from $\mathbb{G}$. When performing encapsulation, the Encap algorithm picks $n_2 = n/n_1$ independent random integers $(r_1, \ldots, r_{n_2})$ from $\mathbb{Z}_p$, then mix-and-match them to generate n pair-wise independent BDH seeds of the form $e(X, Y_i)^{r_j}$. If we set $n_1 = n_2 = \sqrt{n}$, the yielding scheme has mpk of $O(\sqrt{n})$ group elements and ciphertext of $O(\sqrt{n})$ group elements. Scheme 1 and Scheme 2 can be viewed as special cases of the generalized scheme with the parameter choice $(n_1 = 1, n_2 = n)$ and $(n_1 = n, n_2 = 1)$, respectively. Interestingly, we find that the above trade-off method can naturally apply to the KEM schemes proposed in [HK08, Wee10, HJKS10] and the IB-KEM scheme presented in [Gal10]. Particularly, when implementing the trade-off method to the KEM scheme presented in [HJKS10, Section 3], the resulting scheme is exactly the one constructed by Liu et al. [LLLJ11].

Generalized Scheme 2. Observe that one BDH seed $\mathrm{bdh}(A, B, C)$ is determined by three inputs, then mpk and ciphertext can be further shrunk to $O(\sqrt[3]{n})$ group elements by using the mix-and-match method twice. More precisely, instead of generating the BDH seed like $e(X, Y_i)^{r_j}$ as the above generalized scheme, we can generate the BDH seeds of the form $e(Y_i, Y_j)^{r_k}$. That is, first self mix-and-match the set $(Y_1, \ldots, Y_{n_1})$, then mix-and-match the resulting $n_1(n_1-1)/2$ bases $e(Y_i, Y_j)$ $(i \neq j)$ with n_2 random integers $(r_1, \ldots, r_{n_2})$. The self mix-and-match method is better than the "implicitly defining" method used in [HJKS10, Section 5.3] since it travels all the binary combinatorial pairs (Y_i, Y_j) over the set $(Y_1, \ldots, Y_{n_1})$, thus it can generate the same number of bases with smaller mpk. Based on this observation, we propose another generalized scheme called Scheme 4 as follows. The detailed construction and security proof are deferred to Section 7.

$$
\begin{array}{ll}
\mathsf{Setup}: & mpk = (g, h, X, X', Y_1 = g^{y_1}, \ldots, Y_{n_1} = g^{y_{n_1}}), msk = (y_1, \ldots, y_{n_1}) \\
\mathsf{KeyGen}: & sk = (sk_{ij}) \text{ for } 1 \le i < j \le n_1 \text{ where } sk_{ij} = (g^{y_i y_j} F(I)^{s_{ij}}, g^{s_{ij}}) \\
\mathsf{Encap}: & C = (C_1, \ldots, C_{n_2}), \text{ where } C_k = (g^{r_k}, (X^t X')^{r_k}, F(I)^{r_k}) \\
& \text{with } t = \mathsf{TCR}(C_{i,1}, \ldots, C_{n_2,1}) \\
& K = (K_{i,j,k}) \text{ for } 1 \le i < j \le n_1, 1 \le k \le n_2, \text{where } K_{i,j,k} = f_{\mathrm{gl}}(e(Y_i, Y_j)^{r_k}, R)
\end{array}
$$

To generate n pair-wise independent BDH seeds we require that $n = n_1(n_1 - 1)n_2/2$. Let $n_1 = n_2$, then the public parameters and the ciphertext are both of $O(\sqrt[3]{n})$ groups elements. Not surprisingly, this trade-off technique can also apply to the KEM scheme [HJKS10, Section 5.3] and the IB-KEM scheme [Gal10].

Scheme	Assumption	Ciphertext Overhead	Efficiency [# exp, # pairing] Encap	Decap	Key Sizes $\|mpk\|$	$\|msk\|$	$\|sk\|$
Galindo [Gal10]	CBDH	$4 \times \|\mathbb{G}_T\|$	$[4, 0]$	$[2, 2n+2]$	$(2n+9) \times \|\mathbb{G}\|$	$(n+4) \times \|\mathbb{Z}_p\|$	$2n \times \|\mathbb{G}\|$
Scheme 1 (§4)	CBDH	$3n \times \|\mathbb{G}_T\|$	$[3n+1, 0]$	$[1, 4n]$	$5 \times \|\mathbb{G}\|$	$1 \times \|\mathbb{Z}_p\|$	$2 \times \|\mathbb{G}\|$
Scheme 2 (§5)	CBDH	$3 \times \|\mathbb{G}_T\|$	$[4, 0]$	$[1, 2n+2]$	$(n+4) \times \|\mathbb{G}\|$	$1 \times \|\mathbb{Z}_p\|$	$2n \times \|\mathbb{G}\|$
Scheme 3 (§6)	CBDH	$3n_2 \times \|\mathbb{G}_T\|$	$[3n_2+1, 0]$	$[1, 2n+2n_2]$	$(n_1+4) \times \|\mathbb{G}\|$	$1 \times \|\mathbb{Z}_p\|$	$2n_1 \times \|\mathbb{G}\|$
Scheme 4 (§7)	CBDH	$3n_2 \times \|\mathbb{G}_T\|$	$[3n_2+1, 0]$	$[1, 2n+2n_2]$	$(n_1+4) \times \|\mathbb{G}\|$	$n_1 \times \|\mathbb{Z}_p\|$	$2n/n_2 \times \|\mathbb{G}\|$

In Scheme 3 we have $n = n_1 n_2$, then n_1 and n_2 can be set to integers around $O(\sqrt{n})$. In Scheme 4 we have $n_1(n_1-1)n_2/2$, then n_1 and n_2 can be set to integers around $O(\sqrt[3]{n})$.

Table 1. Efficiency comparison of the proposed schemes

1.3 Related Work

Recently, Galindo [Gal10] gave an IND-sID-CCA secure IB-KEM based on the CBDH assumption in the standard model by integrating the KEM scheme [HK08] with the BB_1-IBE scheme [BB04]. Galindo's scheme is not conceptually simple due to the complexity of the underlying KEM scheme [HK08], and its master secret consists of $O(n)$ group elements that might be impractical for some applications. Haralambiev et al. [HJKS10] mentioned that their KEM scheme with public key of size $O(\sqrt{n})$ can extend to selective-identity secure BB_1-IBE scheme [BB04]. They sketched their ideas as follows: the IBE scheme has the same parameters as their KEM scheme [HJKS10, Section 5.3], and a private key for identity I contains $2n$ group elements of the form $(g^{z_i z'_j} \cdot (X^I X')^{s_{ij}}, g^{s_{ij}}) \in \mathbb{G}^2$. However, we remark that a private key for identity I should be $(g^{z_i z'_j} \cdot F(I)^{s_{ij}}, g^{s_{ij}})$, where $F(I)$ is the Boneh-Boyen hash. Besides, the master secret key of their scheme is still a bit large ($2\sqrt{n}$ elements from $\mathbb{Z}_p$), which may render it less practical in use. Regarding to this, it would be very interesting to construct IBE schemes with short master secret key while provably secure under weak assumptions in the standard model.

2 Preliminaries

2.1 Notation

We use standard asymptotic notation O and o to denote the growth of functions. We denote with $\mathsf{poly}(\kappa)$ an unspecified function $f(\kappa) = O(\kappa^c)$ for some constant c. We denote with $\mathsf{negl}(\kappa)$ an unspecified function $f(\kappa)$ such that $f(\kappa) = o(\kappa^{-c})$ for every constant c. Throughout the paper, a *probabilistic polynomial-time* (PPT) algorithm is a randomized algorithm that runs in time $\mathsf{poly}(\kappa)$. For a positive integer n, we denote with $[n]$ the set $[n] = \{1, \ldots, n\}$. For a finite set S, we use $s \xleftarrow{R} S$ to denote that s is sampled from the set S uniformly at random.

2.2 Identity based Key Encapsulation Mechanisms

An identity-based key encapsulation mechanism (IB-KEM) [BFMLS08] consists of four PPT algorithms as follows:

Setup: takes the security parameter 1^κ as input and outputs the public parameter mpk and the master secret msk. Intuitively, mpk is the system parameters which will be public known, while the msk will be known only to the thrusted third party, called Private Key Generator.
KeyGen: takes mpk, msk, an identity I as input and outputs the associated private key sk.
Encap: takes mpk and an identity as input and outputs a pair (C, K) where C is the ciphertext and $K \in \mathcal{K}$ is a data encryption key.

Decap: takes mpk, private key sk, and a ciphertext C as input and outputs the data encryption key $K \in \mathcal{K}$.

We require that if $(mpk, msk) \xleftarrow{R} \mathsf{Setup}(1^\kappa)$, $sk \leftarrow \mathsf{KeyGen}(mpk, msk, I)$, and $(C, K) \leftarrow \mathsf{Encap}(mpk, I)$ then we have $\mathsf{Decap}(mpk, sk, C) = K$.

2.3 Chosen Ciphertext Security

CCA-security of an IB-KEM is defined by the following game playing between an adversary $\mathcal{A}$ and a challenger $\mathcal{CH}$.

Setup. $\mathcal{CH}$ takes a security parameter 1^κ and runs the KeyGen algorithm. It gives the adversary the resulting system parameters. It keeps the master key to itself.
Phase 1. $\mathcal{A}$ may make polynomially-many private key queries and decapsulation queries. $\mathcal{CH}$ answers these queries by running the algorithm KeyGen to extract the associated private keys.
Challenge. Once the adversary decides that Phase 1 is over it outputs an identity I^* on which it wishes to be challenged. The only constraint is that I^* did not appear in any private key extraction query in Phase 1. $\mathcal{CH}$ computes $(C^*, K_0^*) = \mathsf{Encap}(mpk, I^*)$, samples K_1^* uniform randomly from $\mathcal{K}$. Finally, $\mathcal{CH}$ picks a random bit $\beta \in \{0, 1\}$ and sends (C^*, K_β^*) as the challenge to the adversary.
Phase 2. $\mathcal{A}$ issues more private key queries with the restriction that $\langle I \rangle \neq \langle I^* \rangle$ and the decapsulation queries with the restriction that $\langle I, C \rangle \neq \langle I^*, C^* \rangle$.
Guess. Finally, $\mathcal{A}$ outputs a guess $\beta' \in \{0, 1\}$ and wins the game if $\beta = \beta'$.

We refer to such an adversary $\mathcal{A}$ as an $\mathsf{IND\text{-}ID\text{-}CCA}$ adversary. We define adversary $\mathcal{A}$'s advantage over the IB-KEM scheme $\mathcal{E}$ by $\mathrm{Adv}^{\mathsf{CCA}}_{\mathcal{E},\mathcal{A}}(\kappa) = \left|\Pr[\beta = \beta'] - \frac{1}{2}\right|$, where κ is the security parameter. The probability is over the random bits used by the challenger and the adversary.

Definition 2.1 *We say that an IB-KEM scheme $\mathcal{E}$ is* $\mathsf{IND\text{-}ID\text{-}CCA}$ *secure if for any PPT* $\mathsf{IND\text{-}ID\text{-}CCA}$ *adversary $\mathcal{A}$ the advantage* $\mathrm{Adv}^{\mathsf{CCA}}_{\mathcal{E},\mathcal{A}}(\kappa)$ *is negligible.*

Selective-identity CCA-security [CHK04] can be defined in a similar game as the above game of full-identity CCA-security, except that the adversary needs to output a target identity at the very beginning of the game. We refer to such an adversary $\mathcal{A}$ as an $\mathsf{IND\text{-}sID\text{-}CCA}$ adversary. We define adversary $\mathcal{A}$'s advantage over the IB-KEM scheme $\mathcal{E}$ by $\mathrm{Adv}^{\mathsf{CCA}}_{\mathcal{E},\mathcal{A}}(\kappa) = \left|\Pr[\beta = \beta'] - \frac{1}{2}\right|$, where κ is the security parameter. The probability is over the random bits used by the challenger and the adversary.

Definition 2.2 *We say that an IB-KEM scheme $\mathcal{E}$ is* $\mathsf{IND\text{-}sID\text{-}CCA}$ *secure if for any PPT* $\mathsf{IND\text{-}sID\text{-}CCA}$ *adversary $\mathcal{A}$ the advantage* $\mathrm{Adv}^{\mathsf{CCA}}_{\mathcal{E},\mathcal{A}}(\kappa)$ *is negligible.*

2.4 Target Collision Resistant Hash Function

$\mathrm{TCR} = (\mathsf{TCR}_k)_{k \in \mathbb{N}}$ is a family of keyed hash function $\mathsf{TCR}^s_k : \mathbb{G} \to \mathbb{Z}_p$ for each k-bit key s. For an adversary $\mathcal{H}$, its tcr-advantage $\mathrm{Adv}^{\mathrm{TCR}}_{\mathcal{H}}(k)$ is defined as:

$$\Pr[\mathsf{TCR}^s(c^*) = \mathsf{TCR}^s(c) \ \wedge \ c \neq c^* : s \xleftarrow{R} \{0,1\}^k; c^* \xleftarrow{R} \mathbb{G}; c \leftarrow \mathcal{H}(s, c^*)]$$

Note that TCR is a weaker requirement than collision-resistance, so any practical collision-resistant function can be used. To simplify notation we will drop the superscript s and simply use TCR hereafter. Additionally, we can define multi-inputs TCR function in a natural way, that is $\mathsf{TCR}^s_k : (\mathbb{G})^n \to \mathbb{Z}_p$. The corresponding tcr-advantage of an adversary $\mathcal{H}$ is defined in a similar way except substituting c with $(c_1, \ldots, c_n)$ and c^* with $(c_1^*, \ldots, c_n^*)$.

2.5 Computational Bilinear Diffie-Hellman Assumption

Let $\mathbb{G}$ be a cyclic group generated by g and equipped with a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. Define

$$\mathrm{bdh}(A, B, C) := T, \text{ where } A = g^a, B = g^b, C = g^c, \text{ and } T = e(g, g)^{abc}$$

The computational bilinear Diffie-Hellman (CBDH) problem is computing the value $\mathrm{bdh}(A, B, C)$ given random $A, B, C \in \mathbb{G}$. The CBDH assumption asserts that the CBDH problem is hard, that is, $\Pr[\mathcal{A}(A, B, C) = \mathrm{bdh}(A, B, C)] \leq \mathsf{negl}(\kappa)$ for all PPT algorithms $\mathcal{A}$.

In the bilinear setting, the Goldreich-Levin theorem [GL89] gives us the following lemma for a Goldreich-Levin hardcore predicate $f_{\mathrm{gl}} : \mathbb{G}_T \times \{0,1\}^u \to \{0,1\}$.

Lemma 2.3 *Let $\mathbb{G}$ be a prime order group generated by g equipped with a pairing $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. Let $A, B, C \xleftarrow{R} \mathbb{G}$ be random group elements, $R \xleftarrow{R} \{0,1\}^u$, and let $K = f_{\mathrm{gl}}(\mathrm{bdh}(A, B, C), R)$. Let $U \xleftarrow{R} \{0,1\}$ be uniformly random. Suppose there exists a PPT algorithm $\mathcal{B}$ distinguishing the distributions $\Delta_{\mathrm{bdh}} = (g, A, B, C, K, R)$ and $\Delta_{\mathrm{rand}} = (g, A, B, C, U, R)$ with non-negligible advantage. Then there exists a PPT algorithm computing $\mathrm{bdh}(A, B, C)$ on input (A, B, C) with non-negligible success probability, hence breaking the CBDH problem.*

We assume that the global public parameters known to all the parties consist of the pairing parameters $(e, \mathbb{G}, \mathbb{G}_T, g, p) \leftarrow \mathsf{GroupGen}(1^\kappa)$, the descriptions of a target collision resistant hash function TCR and a suitable Goldreich-Levin hardcore predicate $f_{\mathrm{gl}}(\cdot, R)$ with randomness R to extract one pseudorandom bit from a BDH seed. It is well known that an IB-KEM scheme compares favorably to an IBE scheme in many ways [CS01, BFMLS08], and IB-KEM schemes can be readily bootstrapped to full functional IBE schemes by coupling with a DEM having appropriate properties. Therefore in this paper, we focus on the constructions of IB-KEM.

3 A 1-bit IB-KEM Scheme

In this section we describe an 1-bit IB-KEM which is obtained by extending the techniques of [HJKS10] to the Boneh-Boyen IBE scheme [BB04]. The resulting IB-KEM scheme is IND-sID-CCA secure based on the CBDH assumption. It is defined as follows.

Setup. Pick $a \xleftarrow{R} \mathbb{Z}_p$, $h, X', Y \xleftarrow{R} \mathbb{G}$, set $X = g^a$, and define the function $F : \mathbb{Z}_p \to \mathbb{G}$ as $I \mapsto X^I h$. The public parameters and the master secret key are given by

$$mpk = (g, h, X, X', Y) \text{ and } msk = a$$

KeyGen. To generate a private key for an identity $I \in \mathbb{Z}_p$, pick $s \xleftarrow{R} \mathbb{Z}_p$ and output

$$sk = (Y^a F(I)^s, g^s)$$

Encap. Pick $r \xleftarrow{R} \mathbb{Z}_p$, then generate the ciphertext $C = (C_1, C_2, C_3)$ as $C_1 = g^r$, $C_2 = (X^t X')^r$ with $t = \mathsf{TCR}(C_1)$, and $C_3 = F(I)^r$. Compute

$$K = f_{\mathrm{gl}}(e(X, Y)^r, R)$$

Decap. To decapsulate ciphertext (C_1, C_2, C_3) under identity I, first compute $t = \mathsf{TCR}(C_1)$. If $e(C_1, X^t X') \neq e(g, C_2)$ or $e(C_1, F(I)) \neq e(g, C_3)$ then return $\perp$. Take the private key sk and the ciphertext $C = (C_1, C_2, C_3)$ as input and outputs $K = f_{\mathrm{gl}}\left(\frac{e(C_1, sk_1)}{e(C_3, sk_2)}, R\right)$. Indeed, for a valid ciphertext, we have

$$\frac{e(C_1, sk_1)}{e(C_3, sk_2)} = \frac{e(g^r, Y^a F(I)^s)}{e(F(I)^r, g^s)} = e(X, Y)^r.$$

Notice that the consistency of the ciphertext is publicly verifiable, i.e., anyone can verify a ciphertext being consistent or not.

Theorem 3.1 *Let* TCR *be a target collision-resistant hash function and suppose that the CBDH assumption holds in* $\mathbb{G}$*. Then the above scheme is an* $\mathsf{IND\text{-}sID\text{-}CCA}$ *secure IB-KEM.*

Proof. We proceed in a sequence of games. We write (C_1^*, C_2^*, C_3^*) to denote the challenge ciphertext with the corresponding key K^* of identity I^*, denote with U^* the random key chosen by the $\mathsf{IND\text{-}sID\text{-}CCA}$ experiment, and set $t^* = \mathsf{TCR}(C_1^*)$. Let W_i denote the event that $\mathcal{A}$ outputs β' such that $\beta' = \beta$ in Game i.

Game 0. This is the standard $\mathsf{IND\text{-}sID\text{-}CCA}$ game. By definition we have

$$\Pr[W_0] = \frac{1}{2} + \mathsf{AdvCCA}^{\mathcal{A}}_{\mathsf{KEM}}(\kappa) \tag{1}$$

Game 1. Let E_{01} be the event that the adversary issues a decapsulation query $\langle I^*, C_1', C_2', C_3' \rangle$ with $C_1' = C_1^*$ in Phase 1. Note that the probability that the adversary submits a decapsulation query such that $C_1' = C_1^*$ before seeing the challenge ciphertext is bounded by Q_d/p, where Q_d is the number of decapsulation queries issued by $\mathcal{A}$. Since $Q_d = \mathsf{poly}(\kappa)$, we have $\Pr[E_{01}] \leq Q_d/p \leq \mathsf{negl}(\kappa)$. We define Game 1 exactly the same as Game 0 except assuming that E_{01} never occurs in Game 1. It follows that

$$|\Pr[W_1] - \Pr[W_0]| \leq \mathsf{negl}(\kappa) \tag{2}$$

Moreover, we remark that in Phase 2 a decapsulation query $\langle I^*, C_1', C_2', C_3' \rangle$ will be rejected if $C_1' = C_1^*$. Since if $C_2' \neq C_2^*$ or $C_3' \neq C_3^*$, the decapsulation query will be rejected for the inconsistency of the ciphertext. If $C_2' = C_2^*$ and $C_3' = C_3^*$, it will be rejected by definition of $\mathsf{IND\text{-}sID\text{-}CCA}$ game.

Game 2. Let E_{12} be the event that the adversary issues a decapsulation query $\langle I^*, C_1', C_2', C_3' \rangle$ with $C_1' \neq C_1^*$ and $\mathsf{TCR}(C_1') = \mathsf{TCR}(C_1^*)$. By the target collision resistance of TCR, we have $\Pr[E_{12}] \leq \mathsf{negl}(\kappa)$. We define Game 2 exactly the same as Game 1 except assuming that E_{12} never occurs in Game 2. It follows that

$$|\Pr[W_2] - \Pr[W_1]| \leq \mathsf{negl}(\kappa) \tag{3}$$

We claim that

$$\Pr[W_2] = \frac{1}{2} + \mathsf{negl}(\kappa) \tag{4}$$

We prove this statement by letting an adversary against the GL-DBDH assumption simulate the challenger in Game 2. $\mathcal{B}$ is given a challenge instance (g, A, B, C, L, R), where L is either randomly sampled from $\{0,1\}$ or $f_{\mathrm{gl}}(\mathrm{bdh}(A,B,C), R)$. $\mathcal{B}$ plays the game with an adversary $\mathcal{A}$ against the IND-sID-CCA security of the 1-bit IB-KEM scheme.

Initialization. $\mathcal{A}$ first outputs an identity $I^* \in \mathbb{Z}_p$ that it intends to attack.

Setup. $\mathcal{B}$ picks $d \xleftarrow{R} \mathbb{Z}_p$, and then sets $X = A = g^a$, $X' = X^{-t^*} g^d$, $Y = B = g^b$, where $t^* = \mathsf{TCR}(C)$. $\mathcal{B}$ picks $z \xleftarrow{R} \mathbb{Z}_p$ and defines $h = X^{-I^*} g^z$. It gives $\mathcal{A}$ the public parameters $mpk = (g, h, X, X', Y)$. The corresponding msk, which is unknown to $\mathcal{B}$ is a. The function F is essentially of the form

$$F(I) = X^I h = X^{I - I^*} g^z$$

Phase 1 - Private Key Queries. $\mathcal{A}$ issues up to Q_e private key queries with the only restriction that $\langle I \rangle \neq \langle I^* \rangle$. To respond to a private query for identity $I \in \mathbb{Z}_p$, $\mathcal{B}$ generates sk as follows: for sk_ℓ algorithm $\mathcal{B}$ picks $s \xleftarrow{R} \mathbb{Z}_p$ and sets

$$sk_1 = Y^{\frac{-z}{I-I^*}} F(I)^s, \quad sk_2 = g^s Y^{\frac{-1}{I-I^*}}$$

Let $\widetilde{s} = s - b/(I - I^*)$. It is easy to see that sk is a valid random private key for I since

$$sk_1 = Y^{\frac{-z}{I-I^*}} (X^{I-I^*} g^z)^s = Y^a (X^{I-I^*} g^z)^{s - \frac{b}{I-I^*}} = Y^a F(I)^{\widetilde{s}_\ell}$$
$$sk_2 = g^s Y^{\frac{1}{I-I^*}} = g^{\widetilde{s}}$$

where s, $\widetilde{s}$ are uniform in $\mathbb{Z}_p$. This matches the definition for a private key for I. Hence, sk is a valid private key for I.

Phase 1 - Decapsulation Queries. Upon $\mathcal{A}$ issuing a decaptulation query $\langle I, C_1, C_2, C_3 \rangle$, $\mathcal{B}$ responds as follows. If $I \neq I^*$, $\mathcal{B}$ uses the corresponding private key to handle it. Otherwise, $\mathcal{B}$ computes $t = \mathsf{TCR}(C_1)$ and tests the consistency of the ciphertext by checking

$$e(C_1, X^t X') \stackrel{?}{=} e(g, C_2) \ \wedge \ e(C_1, F(I)) \stackrel{?}{=} e(g, C_3)$$

If the equality holds, $\mathcal{B}$ sets $K := f_{\mathrm{gl}}(e(\widetilde{X}, Y), R)$. It is easy to see that the decapsulation result is correct by observing $\widetilde{X} = (C_2/C_1^d)^{1/(t-t^*)} = (X^{r(t-t^*)} g^{rd} / g^{rd})^{1/(t-t^*)} = X^r = \mathrm{dh}(X, C_1)$. By the definition of Game 2 we know that when $I = I^*$, if $C_1 \neq C_1^*$ then we have $t \neq t^*$. Therefore $\mathcal{B}$ can answer all decapsulation queries issued by $\mathcal{A}$ correctly.

Challenge. $\mathcal{B}$ sets $C_1^* = C$ (which implicitly assigns $r = c$), $C_2^* = C^d$, and $C_3^* = C^z$. The challenge ciphertext is $C^* = (C_1^*, C_2^*, C_3^*)$. Note that this is a consistent ciphertext since we have $(X^{t^*} X')^r = (g^d)^r = C^d$ and $F(I^*)^r = (g^z)^r = C^z$. Then $\mathcal{B}$ sets $K^* = L$ and gives $\mathcal{A}$ the challenge (C^*, K^*).

Phase 2. In Phase 2, all the queries are responded in the same way as in Phase 1 except the decapsulation query $\langle I^*, C^* \rangle$ will be rejected.

This finishes the description of simulation. It is easy to see that $\mathcal{B}$ simulates the challenger perfectly. If $\mathcal{A}$'s advantage is not negligible, then $\mathcal{B}$ has non-negligible advantage against the GL-DBDH problem. According to Lemma 2.3, $\mathcal{B}$ further implies an algorithm with non-negligible advantage against the CBDH problem, which contradicts to the CBDH assumption. Therefore, we prove the statement. The theorem follows by combining (1)-(4). □

4 CCA Secure IB-KEM with Constant Size Public Parameters

In this section we present a n-bit IB-KEM scheme based on the 1-bit IB-KEM scheme using multiple encapsulations method.

Setup. The same as Scheme 0.

KeyGen. The same as Scheme 0.

Encap. Pick $r_1, \ldots, r_n \xleftarrow{R} \mathbb{Z}_p$, then compute $C_{i,1} = g^{r_i}$, $t = \mathsf{TCR}(C_{1,1}, \ldots, C_{n,1})$, $C_{i,2} = (X^t X')^{r_i}$, $C_{i,3} = F(I)^{r_i}$. The final ciphertext is $C = (C_1, \ldots, C_n)$, where $C_i = (C_{i,1}, C_{i,2}, C_{i,3})$. Compute $K = (K_1, \ldots, K_n)$, where

$$K_i = f_{\mathrm{gl}}(e(X, Y)^{r_i}, R) \text{ for } 1 \leq i \leq n.$$

Decap. To decapsulate ciphertext $C = (C_1, \ldots, C_n)$ under identity I, first compute $t = \mathsf{TCR}(C_{1,1}, \ldots, C_{n,1})$. If $e(C_{i,1}, X^t X') \neq e(g, C_{i,2})$ or $e(C_{i,1}, F(I)) \neq e(g, C_{i,3})$ for any $i \in [n]$ then return $\perp$. Take the private key $sk = (sk_1, sk_2)$ and the ciphertext $C = (C_1, \ldots, C_n)$ as input and output

$$K_i = f_{\mathrm{gl}}\left(\frac{e(C_{i,1}, sk_1)}{e(C_{i,3}, sk_2)}, R\right) \text{ for } 1 \leq i \leq n.$$

Indeed, for a valid ciphertext, we have

$$\frac{e(C_{i,1}, sk_1)}{e(C_{i,3}, sk_2)} = \frac{e(g^{r_i}, Y^a F(I)^s)}{e(F(I)^{r_i}, g^s)} = e(X, Y)^{r_i} \text{ for } 1 \leq i \leq n.$$

Theorem 4.1 *Let* TCR *be a target collision-resistant hash function and suppose that the CBDH assumption holds in* $\mathbb{G}$*. Then the above scheme is an* $\mathsf{IND\text{-}sID\text{-}CCA}$ *secure IB-KEM.*

The security is somewhat straightforward by conducting the hybrid argument with the proof of Scheme 0. For completeness we put the proof in Appendix B.

5 CCA Secure IB-KEM with Constant Size Ciphertext

In this section we present a n-bit IB-KEM scheme based on the 1-bit IB-KEM scheme using the randomness-reuse technique.

Setup. Pick $a \xleftarrow{R} \mathbb{Z}_p$, $h, X', Y_1, \ldots, Y_n \xleftarrow{R} \mathbb{G}$, set $X = g^a$, and define the function $F : \mathbb{Z}_p \to \mathbb{G}$ as $I \mapsto X^I h$. The mpk and the msk are given by

$$mpk = (g, h, X, X', Y_1, \ldots, Y_n) \text{ and } msk = a$$

KeyGen. To generate a private key for an identity $I \in \mathbb{Z}_p$, pick $s_1, \ldots, s_n \xleftarrow{R} \mathbb{Z}_p$ and output $sk = (sk_1, \ldots, sk_n)$, where

$$sk_i = (Y_i^a F(I)^{s_i}, g^{s_i}) \text{ for } 1 \leq i \leq n.$$

Encap. Pick $r \xleftarrow{R} \mathbb{Z}_p$, then generate the ciphertext $C = (C_1, C_2, C_3)$ as $C_1 = g^r$, $C_2 = (X^t X')^r$ with $t = \mathsf{TCR}(C_1)$, and $C_3 = F(I)^r$. Compute $K = (K_1, \ldots, K_n)$, where

$$K_i = f_{\mathrm{gl}}(e(X, Y_i)^r, R) \text{ for } 1 \leq i \leq n.$$

Decap. To decapsulate ciphertext (C_1, C_2, C_3) under identity I, first compute $t = \mathsf{TCR}(C_1)$. If $e(C_1, X^t X') \neq e(g, C_2)$ or $e(C_1, F(I)) \neq e(g, C_3)$ then return $\perp$. Take the private key $sk = (sk_1, \ldots, sk_n)$ and the ciphertext $C = (C_1, C_2, C_3)$ as input and output

$$K_i = f_{\mathrm{gl}}\left(\frac{e(C_1, sk_{i,1})}{e(C_3, sk_{i,2})}, R\right) \text{ for } 1 \leq i \leq n.$$

Indeed, for a valid ciphertext, we have

$$\frac{e(C_1, sk_{i,1})}{e(C_3, sk_{i,2})} = \frac{e(g^r, Y_i^a F(I)^{s_i})}{e(F(I)^r, g^{s_i})} = e(X, Y_i)^r \text{ for } 1 \leq i \leq n.$$

Notice that the consistency of the ciphertext is publicly verifiable, i.e., anyone could verify a ciphertext being consistent or not.

Theorem 5.1 *Let* TCR *be a target collision-resistant hash function and suppose that the CBDH assumption holds in* $\mathbb{G}$*. Then the above scheme is an* $\mathsf{IND\text{-}sID\text{-}CCA}$ *secure IB-KEM.*

The security is somewhat straightforward by conducting the hybrid argument with the proof of Scheme 0. For completeness we put the proof in Appendix C.

6 Generalized Scheme 1

In this section we present the first generalized scheme which shows that there exists a trade-off between the ciphertext size and the public parameters size. We assume that n is the product of n_1 and n_2. The generalized scheme is defined as follows.

Setup. The same as Scheme 2 except we substitute n with n_1.
KeyGen. The same as Scheme 2 except that we substitute n with n_1.
Encap. Pick $r_1, \ldots, r_{n_2} \xleftarrow{R} \mathbb{Z}_p$, and set $C_{j,1} = g^{r_j}$ for $1 \leq j \leq n_2$. Set $t = \mathsf{TCR}(C_{1,1}, \ldots, C_{n_2,1})$, $C_{j,2} = (X^t X')^{r_j}$, $C_{j,3} = F(I)^{r_j}$ for $1 \leq j \leq n_2$. The ciphertext is $C = (C_1, \ldots, C_{n_2})$ where $C_j = (C_{j,1}, C_{j,2}, C_{j,3})$. Compute the symmetric key $K = (K_1, \ldots, K_n)$, where

$$K_{(i-1)\times n_1 + j} = f_{\mathrm{gl}}(e(X, Y_i)^{r_j}, R) \text{ for } 1 \leq i \leq n_1 \text{ and } 1 \leq j \leq n_2.$$

Decap. To decapsulate ciphertext $C = (C_1, \ldots, C_{n_2})$ encrypted under identity I, first compute $t = \mathsf{TCR}(C_{1,1}, \ldots, C_{n_2,1})$. If $e(C_{j,1}, X^t X') \neq e(g, C_{j,2})$ or $e(C_{j,1}, F(I)) \neq e(g, C_{j,3})$ for some $j \in [n_2]$ then return $\perp$. Take the private key $sk = (sk_1, \ldots, sk_{n_1})$ and $C = (C_1, \ldots, C_{n_2})$ as input and output

$$K_{(i-1)\times n_1 + j} = f_{\mathrm{gl}}\left(\frac{e(C_{j,1}, sk_{i,1})}{e(C_{j,3}, sk_{i,2})}, R\right) \text{ where } 1 \leq i \leq n_1 \text{ and } 1 \leq j \leq n_2.$$

Indeed, for a valid ciphertext, we have

$$\frac{e(C_{j,1}, sk_{i,1})}{e(C_{j,3}, sk_{i,2})} = \frac{e(g^{r_j}, Y_i^a F(I)^{s_i})}{e(F(I)^{r_j}, g^{s_i})} = e(X, Y_i)^{r_j} \text{ for } 1 \leq i \leq n_1 \text{ and } 1 \leq j \leq n_2.$$

Particularly, let n be a perfect square and $n_1 = n_2 = \sqrt{n}$, we obtain an IB-KEM scheme with $O(\sqrt{n})$ public parameters size and $O(\sqrt{n})$ ciphertext size.

Theorem 6.1 *Let* TCR *be a target collision-resistant hash function and suppose that the CBDH assumption holds in* $\mathbb{G}$*. Then the above scheme is an* $\mathsf{IND\text{-}sID\text{-}CCA}$ *secure IB-KEM.*

The security is somewhat straightforward by conducting the hybrid argument with the proof of Scheme 0. For completeness we put the proof in Appendix D.

7 Generalized Scheme 2

In this section we present the second generalized scheme. We assume that $n = n_1(n_1 - 1)n_2/2$.

Setup. mpk and msk are given by

$$mpk = (g, h, X, X', Y_1 = g^{y_1}, \ldots, Y_{n_1} = g^{y_{n_1}}, F) \text{ and } msk = (y_1, \ldots, y_{n_1})$$

KeyGen. To generate a private key $sk = (sk_{ij})$ for an identity $I \in \mathbb{Z}_p$, pick $s_{ij} \xleftarrow{R} \mathbb{Z}_p$ and set $sk_{ij} = (g^{y_i y_j} F(I)^{s_{ij}}, g^{s_{ij}})$ for $1 \leq i < j \leq n_1$.
Encap. Pick $r_1, \ldots, r_{n_2} \xleftarrow{R} \mathbb{Z}_p$, and set $C_{k,1} = g^{r_k}$ for $1 \leq k \leq n_2$. Set $t = \mathsf{TCR}(C_{1,1}, \ldots, C_{n_2,1})$, $C_{j,2} = (X^t X')^{r_j}$, $C_{j,3} = F(I)^{r_j}$ for $1 \leq j \leq n_2$. The ciphertext is $C = (C_1, \ldots, C_{n_2})$ where $C_k = (C_{k,1}, C_{k,2}, C_{k,3})$. Compute the symmetric key $K = (K_{i,j,k})$, where

$$K_{i,j,k} = f_{\mathrm{gl}}(e(Y_i, Y_j)^{r_k}, R) \text{ for } 1 \leq i < j \leq n_1 \text{ and } 1 \leq k \leq n_2.$$

Decap. To decapsulate ciphertext $C = (C_1, \ldots, C_{n_2})$ encrypted under identity I, first compute $t = \mathsf{TCR}(C_{1,1}, \ldots, C_{n_2,1})$. If $e(C_{k,1}, X^t X') \neq e(g, C_{k,2})$ or $e(C_{k,1}, F(I)) \neq e(g, C_{k,3})$ for some $k \in [n_2]$ then return $\perp$. Take the private key $sk = (sk_{ij})$ and $C = (C_1, \ldots, C_{n_2})$ as input and output

$$K_{i,j,k} = f_{\mathrm{gl}}\left(\frac{e(C_{k,1}, sk_{ij,1})}{e(C_{k,3}, sk_{ij,2})}, R\right) \text{ where } 1 \leq i < j \leq n_1 \text{ and } 1 \leq k \leq n_2.$$

Indeed, for a valid ciphertext, we have

$$\frac{e(C_{k,1}, sk_{ij,1})}{e(C_{k,3}, sk_{ij,2})} = \frac{e(g^{r_k}, g^{y_i y_j} F(I)^{s_{ij}})}{e(F(I)^{r_k}, g^{s_{ij}})} = e(Y_i, Y_j)^{r_k} \text{ for } 1 \leq i < j \leq n_1, 1 \leq k \leq n_2.$$

Theorem 7.1 *Let* TCR *be a target collision-resistant hash function and suppose that the CBDH assumption holds in* $\mathbb{G}$*. Then the above scheme is an* $\mathsf{IND\text{-}sID\text{-}CCA}$ *secure IB-KEM.*

The proof is similar to that of Scheme 1 in Section 4, Scheme 2 in Section 5, and Generalized Scheme 1 in Section 6, except that for a given CBDH challenge instance (A, B, C) the reduction algorithm first sets $Y_i = A$ for some $i \in [n_1]$ then sets $X = A^h$ for a random chosen exponent h instead of directly setting $X = A$ as before. For the limit of space, we omit the details here.

8 Extensions

Since BB_1-IBE [BB04] and Waters-IBE [Wat05] share the same commutative-blinding framework, thus we can enhance our IB-KEM schemes with only selective-identity security to IB-KEM schemes with full-identity security by using the Waters-IBE as the underlying IBE scheme. The security proofs are somewhat straightforward by composing the proofs for IB-KEM schemes in Section 4, 5, and 6 based on BB_1-IBE and the proofs for Waters-IBE [Wat05, KG06]. For a concrete example, we sketch the proof of Scheme 1*, which is the resulting scheme of replacing the underlying IBE scheme of Scheme 1 with Waters-IBE, as follows. The proof is conducted by a sequence of games. Game 0 is the standard $\mathsf{IND\text{-}ID\text{-}CCA}$ game. Game 1 is defined like Game 1 except that the reduction algorithm will terminate the simulation due to regular abort or artificial abort. Game 2, Game 3, and Game 4 are defined like Game 1, Game 2, and Game 3 in the proof for Scheme 1, respectively. The argument of the indistinguishability between Game 3 and Game 4 is similar to that between Game 2 and Game 3 in the proof for Scheme 1. Then the security result immediately follows.

Acknowledgments

We would like to thank Jiang Zhang, Cheng Chen, and Qiong Huang for helpful discussions. The work of the third author is supported in part by the National Natural Science Foundation of China under grant Nos. 60970110, 61033014, 61021004, 61170227, 61172085, 61103221, 11061130539 and 61161140320 and Science Foundation Project of Jiang Su Province under grant No. BM20101014.

References

BB04. Dan Boneh and Xavier Boyen. Efficient selective-id secure identity based encryption without random oracles. In *Advances in Cryptology - EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 223–238, 2004.

BFMLS08. Kamel Bentahar, Pooya Farshim, John Malone-Lee, and Nigel P. Smart. Generic constructions of identity-based and certificateless kems. *Journal of Cryptology*, 21(2):178–199, 2008.

BMW05. Xavier Boyen, Qixiang Mei, and Brent Waters. Direct chosen ciphertext security from identity-based techniques. *ACM CCS 2005*, pages 320–329, 2005.

CHK04. Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-ciphertext security from identity based encryption. In *Advances in Cryptology - EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 207–222, 2004.

CHK10. Ronald Cramer, Dennis Hofheinz, and Eike Kiltz. A twist on the naor-yung paradigm and its application to efficient cca-secure encryption from hard search problems. In *Theory of Cryptography, 7th Theory of Cryptography Conference, TCC 2010*, volume 5978 of *LNCS*, pages 146–164. Springer, 2010.

CKS08. David Cash, Eike Kiltz, and Victor Shoup. The twin diffie-hellman problem and applications. In *Advances in Cryptology - EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 127–145, 2008.

CS98. Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *Advances in Cryptology - CRYPTO 1998*, volume 1462 of *LNCS*, pages 13–25, 1998.

CS01. Ronald Cramer and Victor Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. *SIAM Journal on Computing*, 33:167–226, 2001.

CS02. Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In *Advances in Cryptology - EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 45–64. Springer, 2002.

Gal10. David Galindo. Chosen-ciphertext secure identity-based encryption from computational bilinear diffie-hellman. In *Pairing-Based Cryptography - Pairing 2010*, volume 6487 of *LNCS*, pages 367–376. Springer, 2010.

GL89. Oded Goldreich and Leonid A. Levin. A hard-core predicate for all one-way functions. In *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing, STOC*, pages 25–32. ACM, 1989.

HJKS10. Kristiyan Haralambiev, Tibor Jager, Eike Kiltz, and Victor Shoup. Simple and efficient public-key encryption from computational diffie-hellman in the standard model. In *Public Key Cryptography - PKC 2010*, volume 6056 of *LNCS*, pages 1–18. Springer, 2010.

HK07. Dennis Hofheinz and Eike Kiltz. Secure hybrid encryption from weakened key encapsulation. In *Advances in Cryptology - CRYPTO 2007*, volume 4622 of *LNCS*, pages 553–571. Springer, 2007.

HK08. Goichiro Hanaoka and Kaoru Kurosawa. Efficient chosen ciphertext secure public key encryption under the computational diffie-hellman assumption. In *Advances in Cryptology - ASIACRYPT 2008*, volume 5350 of *LNCS*, pages 308–325. Springer, 2008.

HK09. Dennis Hofheinz and Eike Kiltz. Practical chosen ciphertext secure encryption from factoring. In *Advances in Cryptology - EUROCRYPT 2009*, volume 5479 of *LNCS*, pages 313–332. Springer, 2009.

KD04. Kaoru Kurosawa and Yvo Desmedt. A new paradigm of hybrid encryption scheme. In *Advances in Cryptology - CRYPTO 2004*, volume 3152 of *LNCS*, pages 426–442. Springer, 2004.

KG06. Eike Kiltz and David Galindo. Direct Chosen-Ciphertext Secure Identity-Based Key Encapsulation Without Random Oracles. In *Information Security and Privacy, 11th Australasian Conference, ACISP 2006*, volume 4058 of *LNCS*, pages 336–347, 2006.

Kil06. Eike Kiltz. Chosen-ciphertext security from tag-based encryption. In *Theory of Cryptography, TCC 2006*, volume 3876 of *LNCS*, pages 581–600. Springer, 2006.

Kil07. Eike Kiltz. Chosen-ciphertext secure key-encapsulation based on gap hashed diffie-hellman. In *Public Key Cryptography - PKC 2007*, volume 4450 of *LNCS*, pages 282–297. Springer, 2007.

KV08. Eike Kiltz and Yevgeniy Vahlis. Cca2 secure ibe: Standard model efficiency through authenticated symmetric encryption. In *CT-RSA*, volume 4964 of *LNCS*, pages 221–238. Springer, 2008.

LLLJ11. Yamin Liu, Bao Li, Xianhui Lu, and Dingding Jia. Efficient cca-secure cdh based kem balanced between ciphertext and key. In *Information Security and Privacy - 16th Australasian Conference, ACISP 2011*, volume 6812 of *Lecture Notes in Computer Science*, pages 310–318. Springer, 2011.

NY90. Moni Naor and Moti Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *Proceedings of the Twenty Second Annual ACM Symposium on Theory of Computing - STOC*, pages 427–437. ACM, 1990.

Wat05. Brent Waters. Efficient identity-based encryption without random oracles. In *Advances in Cryptology - EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 114–127, 2005.

Wee10. Hoeteck Wee. Efficient chosen-ciphertext security via extractable hash proofs. In *Advances in Cryptology - CRYPTO 2010*, volume 6223 of *LNCS*, pages 314–332. Springer, 2010.

A A Variant of Scheme 0

In this section we describe a variant of Scheme 0 with shorter mpk and ciphertext at the cost of relying on a slightly strong assumption, named the modified computational bilinear Diffie-Hellman assumption.

A.1 The Modified Computational Bilinear Diffie-Hellman Assumption

Let $\mathbb{G}$ be a cyclic group generated by g and equipped with a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. Define

$$\text{mbdh}(A, B, B', C) := T, \text{ where } A = g^a, B = g^b, B' = g^{b^2}, C = g^c, \text{ and } T = e(g, g)^{abc}$$

The modified computational BDH (mCBDH) problem is computing the value $\text{mbdh}(A, B, B', C)$ given $A, B, B', C \in \mathbb{G}$ where $a, b, c \xleftarrow{R} \mathbb{Z}_p$. Compared to the BDH problem, the mBDH problem furthermore provide the adversary with the element g^{b^2}. The mCBDH assumption asserts that the mCBDH problem is hard, that is, $\Pr[\mathcal{A}(A, B, B', C) = \text{mbdh}(A, B, B', C)] \leq \mathsf{negl}(\kappa)$ for all PPT algorithms $\mathcal{A}$.

Lemma 1.1 *Let $\mathbb{G}$ be a prime order group generated by g equipped with a pairing $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. Let $a, b, c \xleftarrow{R} \mathbb{Z}_p$ be random integers, $R \xleftarrow{R} \{0,1\}^u$, and let $K = f_{\text{gl}}(\text{bdh}(A, B, C), R)$. Let $U \xleftarrow{R} \{0,1\}$ be uniformly random. Suppose there exists a PPT algorithm $\mathcal{B}$ distinguishing the distributions*

$$\Delta_{\text{mbdh}} = (g, A, B, B', C, K, R) \text{ and } \Delta_{\text{rand}} = (g, A, B, B', C, U, R)$$

with non-negligible advantage. Then there exists a PPT algorithm computing $\text{bdh}(A, B, C)$ on input (g, A, B, B', C) with non-negligible success probability, hence breaking the mCBDH assumption.

Setup. Pick $a \xleftarrow{R} \mathbb{Z}_p$, and then set $X = g^a$. Pick $h, Y \xleftarrow{R} \mathbb{G}$. Define the function $F : \mathbb{Z}_p \to \mathbb{G}$ as $I \mapsto X^I h$. The public parameters and the master secret key are given by

$$mpk = (g, h, X, Y) \text{ and } msk = a$$

KeyGen. To generate a private key for an identity $I \in \mathbb{Z}_p$, pick $s \xleftarrow{R} \mathbb{Z}_p$ and output $sk = (Y^a F(I)^s, g^{-s}, Y^s)$.
Encap. Pick $r \xleftarrow{R} \mathbb{Z}_p$, then compute $C_1 = g^r$, $C_2 = (F(I)Y^t)^r$ with $t = \mathsf{TCR}(C_1)$. Compute $K = f_{\text{gl}}(e(X, Y)^r, R)$.
Decap. To decapsulate ciphertext (C_1, C_2) under identity I, first compute $t = \mathsf{TCR}(C_1)$. If $e(C_1, F(I)Y^t) \neq e(g, C_2)$ then return $\perp$. Otherwise, take the private key sk and $C = (C_1, C_2)$ as input, compute $K = f_{\text{gl}}\big(e(C_1, sk_1 sk_3^t)e(C_2, sk_2), R\big)$. Indeed, for a valid ciphertext $C = (C_1, C_2)$, we have

$$e(C_1, sk_1 sk_3^t)e(C_2, sk_2) = e(g^r, Y^a F(I)^s Y^{st})e(F(I)^r Y^{rt}, g^{-s}) = e(X, Y)^r$$

Notice that the consistency of the ciphertext is publicly verifiable, i.e., anyone could verify a ciphertext being consistent or not.

Theorem 1.2 *Let TCR be a target collision-resistant hash function and suppose that the mCBDH assumption holds in $\mathbb{G}$. Then the above scheme is an $\mathsf{IND\text{-}sID\text{-}CCA}$ secure IB-KEM.*

Proof. We proceed in a sequence of games. We write (C_1^*, C_2^*) to denote the challenge ciphertext with the corresponding key K^* of identity I^*, denote with U^* the random key chosen by the $\mathsf{IND\text{-}sID\text{-}CCA}$ experiment, and set $t^* = \mathsf{TCR}(C_1^*)$. Let W_i denote the event that $\mathcal{A}$ outputs β' such that $\beta' = \beta$ in Game i.

Game 0. This is the standard IND-sID-CCA game. By definition we have

$$\Pr[W_0] = \frac{1}{2} + \mathsf{AdvCCA}^{\mathcal{A}}_{\mathsf{KEM}}(\kappa) \tag{5}$$

Game 1. Let E_{01} be the event that the adversary issues a decapsulation query $\langle I^*, C_1', C_2' \rangle$ with $C_1' = C_1^*$ in Phase 1. Note that the probability that the adversary submits a decapsulation query such that $C_1' = C_1^*$ before seeing the challenge ciphertext is bounded by Q_d/p, where Q_d is the number of decapsulation queries issued by $\mathcal{A}$. Since $Q_d = \mathsf{poly}(\kappa)$, we have $\Pr[E_{01}] \leq Q_d/p \leq \mathsf{negl}(\kappa)$. We define Game 1 exactly the same as Game 0 except assuming that E_{01} never occurs in Game 1. It follows that

$$|\Pr[W_1] - \Pr[W_0]| \leq \mathsf{negl}(\kappa) \tag{6}$$

Moreover, we remark that in Phase 2 a decapsulation query $\langle I^*, C_1', C_2' \rangle$ will be rejected if $C_1' = C_1^*$. Since if $C_2' \neq C_2^*$, the decapsulation query will be rejected for the inconsistency of the ciphertext. If $C_2' = C_2^*$, it will be rejected by definition of IND-sID-CCA game.

Game 2. Let E_{12} be the event that the adversary issues a decapsulation query $\langle I^*, C_1', C_2' \rangle$ with $C_1' \neq C_1^*$ and $\mathsf{TCR}(C_1') = \mathsf{TCR}(C_1^*)$. By the target collision resistance of TCR, we have $\Pr[E_{12}] \leq \mathsf{negl}(\kappa)$. We define Game 2 exactly the same as Game 1 except assuming that E_{12} never occurs in Game 2. It follows that

$$|\Pr[W_2] - \Pr[W_1]| \leq \mathsf{negl}(\kappa) \tag{7}$$

We claim that

$$\Pr[W_2] = \frac{1}{2} + \mathsf{negl}(\kappa) \tag{8}$$

We prove this statement by letting an algorithm $\mathcal{B}$ against the GL-mDBDH assumption simulate the challenger in Game 2. Suppose $\mathcal{B}$ is given a challenge instance (g, A, B, B', C, L, R), where L is either uniform randomly sampled from $\{0,1\}$ or $f_{\mathrm{gl}}(\mathrm{mbdh}(A, B, B', C), R)$. $\mathcal{B}$ plays Game 2 with an adversary $\mathcal{A}$ against the IB-KEM scheme as follows.

Initialization. $\mathcal{A}$ first outputs an identity $I^* \in \mathbb{Z}_p$ that it intends to attack.

Setup. $\mathcal{B}$ picks $d \xleftarrow{R} \mathbb{Z}_p$, and then sets $X = A = g^a, Y = B = g^b$, compute $t^* = \mathsf{TCR}(C)$. $\mathcal{B}$ picks $d \xleftarrow{R} \mathbb{Z}_p$ and defines $h = X^{-I^*} Y^{-t^*} g^d$. It gives $\mathcal{A}$ the public parameters $mpk = (g, h, X, Y)$. The corresponding msk, which is unknown to $\mathcal{B}$ is a. The function F is essentially of the form

$$F(I) = X^I h = X^{I-I^*} Y^{-t^*} g^d$$

Phase 1 - Private Key Queries. $\mathcal{A}$ issues up to Q_e private key queries with the only restriction that $\langle I \rangle \neq \langle I^* \rangle$. To respond to a private query for identity $I \in \mathbb{Z}_p$, $\mathcal{B}$ generates sk as follows: pick a random integer $s \in \mathbb{Z}_p$ and sets

$$sk_1 = Y^{\frac{-d}{I-I^*}} B'^{\frac{t^*}{I-I^*}} (X^{I-I^*} Y^{-t^*} g^d)^s, sk_2 = g^{-s} Y^{\frac{1}{I-I^*}}, sk_3 = Y^s B'^{\frac{-1}{I-I^*}}$$

Let $\widetilde{s} = s - b/(I - I^*)$. It is easy to see that sk is a valid private key for I since

$$\begin{aligned}
sk_1 &= Y^{\frac{-d}{I-I^*}} B'^{\frac{t^*}{I-I^*}} (X^{I-I^*} Y^{-t^*} g^d)^s = Y^a (X^{I-I^*} Y^{-t^*} g^d)^{s - \frac{b}{I-I^*}} = Y^a F(I)^{\widetilde{s}} \\
sk_2 &= g^{-s} Y^{\frac{1}{I-I^*}} = g^{-s + \frac{b}{I-I^*}} = g^{-\widetilde{s}} \\
sk_3 &= Y^s B'^{\frac{-1}{I-I^*}} = Y^{s - \frac{b}{I-I^*}} = Y^{\widetilde{s}}
\end{aligned}$$

where s, $\widetilde{s}$ are uniform in $\mathbb{Z}_p$. This matches the definition for a private key for I. Hence, sk is a valid private key for I.

Phase 1 - Decapsulation Queries. Upon $\mathcal{A}$ issuing a decaptulation query $\langle I, C_1, C_2\rangle$, $\mathcal{B}$ responds as follows. If $I \neq I^*$, $\mathcal{B}$ uses the corresponding private key to handle it. Otherwise, $\mathcal{B}$ computes $t = \mathsf{TCR}(C_1)$ and tests the consistency of the ciphertext by checking

$$e(C_1, F(I)Y^t) \stackrel{?}{=} e(g, C_2)$$

If the above equality holds, $\mathcal{B}$ sets $K := f_{\mathrm{gl}}(e(\widetilde{Y}, X), R)$. It is easy to verify that the answer is correct by observing that $\widetilde{Y} = (C_2/(C_1^d)^{\frac{1}{d(t-t^*)}} = (Y^{(t-t^*)r}g^{dr}/g^{rd})^{\frac{1}{d(t-t^*)}} = Y^r = \mathrm{dh}(Y, g^r)$. By Game 2 we know that when $I = I^*$, if $C_1 \neq C_1^*$ then $t \neq t^*$. Therefore $\mathcal{B}$ can answer all decapsulation queries issued by $\mathcal{A}$ correctly.
Challenge. $\mathcal{B}$ sets $C_1^* = C$ (which implicitly assigns $r = c$), and $C_2^* = C^d$. The challenge ciphertext is $C^* = (C_1^*, C_2^*)$. Note that this is a consistent ciphertext since we have $(F(I^*)Y^{t^*})^r = (g^d)^r = C^d$. Then $\mathcal{B}$ sets $K^* = L$ and gives $\mathcal{A}$ the challenge (C^*, K^*).
Phase 2. In Phase 2, all the queries are responded in the same way as in Phase 1 except the decapsulation query $\langle I^*, C^*\rangle$ will be rejected.

This finishes the description of simulation. It is easy to see that $\mathcal{B}$ simulates the challenger perfectly. If $\mathcal{A}$'s advantage is not negligible, then $\mathcal{B}$ has non-negligible advantage against the GL-mDBDH problem. According to Lemma 2.3, $\mathcal{B}$ further implies an algorithm with non-negligible advantage against the mCBDH problem, which contradicts to the mCBDH assumption. Therefore, we prove the statement. The theorem follows by combining (5)-(8). □

We compare Scheme 0 and Scheme 0′ in Table 2. Scheme 0′ can be extended to n-bits IB-KEMs in an analogous way as we did to Scheme 0.

Scheme	Assumption	Ciphertext Overhead	Efficiency [# exp, # pairing] Encap	Decap	Key Sizes $\lvert mpk\rvert$	$\lvert msk\rvert$	$\lvert sk\rvert$
Scheme 0 (§3)	CBDH	$3 \times \lvert\mathbb{G}_T\rvert$	$[4, 0]$	$[1, 4]$	$5 \times \lvert\mathbb{G}\rvert$	$1 \times \lvert\mathbb{Z}_p\rvert$	$2 \times \lvert\mathbb{G}\rvert$
Scheme 0′ (§A)	mCBDH	$2 \times \lvert\mathbb{G}_T\rvert$	$[3, 0]$	$[2, 4]$	$4 \times \lvert\mathbb{G}\rvert$	$1 \times \lvert\mathbb{Z}_p\rvert$	$3 \times \lvert\mathbb{G}\rvert$

Table 2. Comparison of Scheme 0 and Scheme 0'

B The Proof of Scheme 1

Proof. We proceed in a sequence of games. Let $(C_1^*, \ldots, C_n^*)$ be the challenge ciphertext of the corresponding key K^* under I^*, denote with U^* the random key chosen by the IND-sID-CCA experiment, and set $t^* = \mathsf{TCR}(C_{1,1}^*, \ldots, C_{n,1}^*)$. We start with a game where the challenger proceeds like the standard IND-sID-CCA game (i.e., K^* is a real key and U^* is a random key), and end up with a game where both K^* and U^* are chosen uniformly random. Then we show that all games are computationally indistinguishable under the CBDH assumption. Let W_i denote the event that $\mathcal{A}$ outputs β' such that $\beta' = \beta$ in Game i.

Game 0. This is the standard IND-sID-CCA game. By definition we have

$$\Pr[W_0] = \frac{1}{2} + \mathsf{AdvCCA}_{\mathsf{KEM}}^{\mathcal{A}}(\kappa)$$

Game 1. Let E_{01} be the event that the adversary issues a decapsulation query $\langle I^*, C_1', \ldots, C_n'\rangle$ with $C_{i,1}' = C_{i,1}^*$ for all $1 \leq i \leq n$ in Phase 1. Note that the probability that the adversary submits a ciphertext such that $C_{i,1}' = C_{i,1}^*$ for all $1 \leq i \leq n$ before seeing the challenge ciphertext

is bounded by Q_d/p^n, where Q_d is the number of decapsulation queries issued by $\mathcal{A}$. Since $Q_d = \mathsf{poly}(\kappa)$, we have $\Pr[E_{0,1}] \leq Q_d/p^n \leq \mathsf{negl}(\kappa)$. We define Game 1 like Game 0 except assuming that E_{01} never occurs in Game 1. It follows that

$$|\Pr[W_1] - \Pr[W_0]| \leq \mathsf{negl}(\kappa)$$

Moreover, we remark that in Phase 2 a decapsulation query $\langle I^*, C'_1, \ldots, C'_n \rangle$ will be rejected if $C'_{i,1} = C^*_{i,1}$ for all $1 \leq i \leq n$. Since if $C'_{i,2} \neq C^*_{i,2}$ or $C'_{i,3} \neq C^*_{i,3}$ for some $i \in [n]$, the decapsulation query will be rejected for the inconsistency of the ciphertext. If $C'_{i,2} = C^*_{i,2}$ and $C'_{i,3} = C^*_{i,3}$ for all $1 \leq i \leq n$, it will be rejected by definition of $\mathsf{IND\text{-}sID\text{-}CCA}$ game.

Game 2. Let E_{12} be the event that the adversary issues a decapsulation query $\langle I^*, C'_1, \ldots, C'_n \rangle$ with $C'_{i,1} \neq C^*_{i,1}$ for some $i \in [n]$ and $\mathsf{TCR}(C'_{1,1}, \ldots, C'_{n,1}) = \mathsf{TCR}(C^*_{1,1}, \ldots, C^*_{n,1})$. By the target collision resistance of TCR we have $\Pr[E_{12}] \leq \mathsf{negl}(\kappa)$. We define Game 2 like Game 1 except assuming that E_{12} never occurs in Game 2. It follows that

$$|\Pr[W_2] - \Pr[W_1]| \leq \mathsf{negl}(\kappa)$$

Game 3. We define Game 3 like Game 2, except that we sample $K^* \xleftarrow{R} \{0,1\}^{n\nu}$ uniformly at random. Note that both K^* and U^* are chosen uniformly random, thus we have

$$\Pr[W_3] = \frac{1}{2}$$

We claim that $|\Pr[W_3] - \Pr[W_2]| \leq \mathsf{negl}(\kappa)$under the CBDH assumption. We prove this by a hybrid argument. To this end, we define a sequence of hybrid games $H_0, \ldots, H_n$, such that H_0 equals Game 2 and H_n equals Game 3. Then we argue that hybrid H_i is indistinguishable from hybrid H_{i-1} for $i \in \{1, \ldots, n\}$ under the CBDH assumption. The claim follows, since $n = n(\kappa)$ is a polynomial. We define H_0 exactly like Game 2. Then, for i from 1 to n, in hybrid H_i we set the first $i\nu$ bits of K^* to independent random bits, and proceed otherwise exactly like in hybrid H_{i-1}. Thus, hybrid H_n proceeds exactly like Game 3. Let E_i denote the event that $\mathcal{A}$ outputs β' such that $\beta' = \beta$ in H_i. Suppose that

$$|\Pr[E_0] - \Pr[E_n]| = 1/\mathsf{poly}'(\kappa) \tag{9}$$

that is, the success probability of $\mathcal{A}$ in H_0 is not negligible close to the success probability in H_n. Note that then there must exist an index i such that $|\Pr[E_{i-1}] - \Pr[E_i]| = 1/\mathsf{poly}(\kappa)$ (since if $|\Pr[E_{i-1}] - \Pr[E_i]| \leq \mathsf{negl}(\kappa)$ for all i, then we should have $|\Pr[E_0] - \Pr[E_n]| \leq \mathsf{negl}(\kappa)$).

Suppose that there exists an algorithm $\mathcal{A}$ for which Equation (9) holds. Then we can construct an adversary $\mathcal{B}$ distinguishing the distributions Δ_{bdh} and Δ_{rand}, which by Lemma 2.3 is sufficient to prove security under the CBDH assumption in $\mathbb{G}$. Adversary $\mathcal{B}$ receives a challenge $D = (g, A, B, C, L, R)$ as input, guesses an index $\ell \in [n]$, which with probability at least $1/n$ such that $|\Pr[E_{\ell-1}] - \Pr[E_\ell]| = 1/\mathsf{poly}(\kappa)$, and proceeds as follows:

Initialization. $\mathcal{A}$ first outputs an identity $I^* \in \mathbb{Z}_p$ that it intends to attack.

Setup. For $i = [n] \backslash \ell$, $\mathcal{B}$ picks $r_i \xleftarrow{R} \mathbb{Z}_p$, then picks $d \xleftarrow{R} \mathbb{Z}_p$, and sets $X = A = g^a$, $Y = B = g^b$, and $X' = X^{-t^*} g^d$, where $t^* = \mathsf{TCR}(g^{r_1}, \ldots, g^{r_{\ell-1}}, C, g^{r_{\ell+1}}, \ldots, g^{r_n})$. Pick $z \xleftarrow{R} \mathbb{Z}_p$ and defines $h = X^{-I^*} g^z$. It gives $\mathcal{A}$ the system parameters $mpk = (g, h, X, X', Y, F)$. Note that the corresponding msk, which is unknown to $\mathcal{B}$ is a.

Phase 1 - Private Key Queries. $\mathcal{A}$ issues up to Q_e private key queries with the only restriction that $\langle I \rangle \neq \langle I^* \rangle$. To respond to a private query of $I \in \mathbb{Z}_p$, $\mathcal{B}$ picks $s \xleftarrow{R} \mathbb{Z}_p$ and sets

$$sk_1 = Y^{\frac{-z}{I-I^*}} F(I)^s, \quad sk_2 = g^s Y^{\frac{-1}{I-I^*}}$$

We claimed that sk is a valid private key for I. To see this, let $\widetilde{s} = s - b/(I - I^*)$. Then we have

$$sk_1 = Y^{\frac{-z}{I-I^*}}(X^{I-I^*}g^z)^s = Y^a(X^{I-I^*}g^z)^{s-\frac{b}{I-I^*}} = Y^a F(I)^{\widetilde{s}}$$
$$sk_2 = g^s Y^{\frac{-1}{I-I^*}} = g^{\widetilde{s}}$$

where s, $\widetilde{s}$ are uniform distributed in $\mathbb{Z}_p$. This matches the definition for a private key for I. Hence, sk is a valid private key for I.

Phase 1 - Decapsulation Queries. Upon $\mathcal{A}$ issuing a decaptulation query $\langle I, C_1, \ldots, C_n\rangle$, $\mathcal{B}$ responds as follows. If $I \neq I^*$, $\mathcal{B}$ uses the corresponding private key to handle it. Otherwise, $\mathcal{B}$ computes $t = \mathsf{TCR}(C_{1,1}, \ldots, C_{n,1})$ and tests the consistency of the ciphertext by checking

$$e(C_{i,1}, X^t X') \stackrel{?}{=} e(g, C_{i,2}) \ \wedge \ e(C_{i,1}, F(I)) \stackrel{?}{=} e(g, C_{i,3})$$

If the equality holds for all $1 \leq i \leq n$, $\mathcal{B}$ sets $K = (K_1, \ldots, K_n)$ as $K_i = f_{\mathrm{gl}}(e(X,Y)^{r_i}, R)$ for $i \in [n]\backslash\{\ell\}$ and $K_\ell = f_{\mathrm{gl}}(e(\widetilde{X_\ell}, Y), R)$. Here we compute $\widetilde{X_\ell} := (C_{\ell,2}/C_{\ell,1}^d)^{1/(t-t^*)} = (X^{r_\ell(t-t^*)}g^{r_i d}/g^{r_i d})^{1/(t-t^*)} = X^{r_\ell} = \mathrm{dh}(X, C_{\ell,1})$. By the definition of Game 2 we know that when $I = I^*$, if $C_{i,1} \neq C^*_{i,1}$ for some $i \in [n]$ then $t \neq t^*$. Therefore $\mathcal{B}$ can answer all decapsulation queries issued by $\mathcal{A}$ correctly.

Challenge. To generate the challenge ciphertext $C^* = (C_1^*, \ldots, C_n^*)$, for $i = [n]\backslash\{\ell\}$, $\mathcal{B}$ generates C_i^* normally. For $C_\ell^* = (C^*_{\ell,1}, C^*_{\ell,2}, C^*_{\ell,3})$, $\mathcal{B}$ sets $C^*_{\ell,1} = C$ (which implicitly assigns $r_\ell = c$), $C^*_{i,2} = C^d$, and $C^*_{i,3} = C^z$. Note that C^* is a consistent ciphertext since we have $(X^{t^*}X')^{r_\ell} = (g^d)^{r_\ell} = C^d$ and $F(I^*)^c = (g^z)^c = C^z$. Then $\mathcal{B}$ samples $\ell - 1$ uniformly random groups of ν bits $K_1^*, \ldots, K_{\ell-1}^*$, sets $K_\ell^* = L$, $K_i^* = f_{\mathrm{gl}}(e(X,Y)^{r_j^*}, R)$ for i from $\ell+1$ to n. $\mathcal{B}$ samples uniform randomly bits $U^* \in \{0,1\}^{n\nu}$, picks a random bit $\beta \in \{0,1\}$. If $\beta = 1$, it gives $\mathcal{A}$ the challenge (C^*, K^*). Otherwise it gives $\mathcal{A}$ the challenge (C^*, U^*).

Phase 2. In Phase 2, all the queries are responded the same way as in Phase 1 except the decapsulation query $\langle I^*, C^*\rangle$ will be rejected.

This completes the description of simulation. If $D \in \Delta_{\mathrm{bdh}}$ we have $K_\ell^* = f_{\mathrm{gl}}(\mathrm{bdh}(A,B,C), R)$. Thus $\mathcal{A}$'s view when interacting with $\mathcal{B}$ is identical to $H_{\ell-1}$. If $D \in \Delta_{\mathrm{rand}}$, then $\mathcal{A}$'s view is identical to H_ℓ. Thus $\mathcal{B}$ can use $\mathcal{A}$ to distinguish $D \in \Delta_{\mathrm{bdh}}$ from $D \in \Delta_{\mathrm{rand}}$. According to Lemma 2.3, $\mathcal{B}$ further implies a PPT algorithm which can break the CBDH problem, which contradicts to the CBDH assumption. □

C The proof of Scheme 2

Proof. We proceed in a sequence of games. We write (C_1^*, C_2^*, C_3^*) to denote the challenge ciphertext with the corresponding key K^* of identity I^*, denote with U^* the random key chosen by the IND-sID-CCA experiment, and set $t^* = \mathsf{TCR}(C_1^*)$. We start with a game where the challenger proceeds like the standard IND-sID-CCA game (i.e., K^* is a real key and U^* is a random key), and end up with a game where both K^* and U^* are chosen uniformly random. Then we show that all games are computationally indistinguishable under the CBDH assumption. Let W_i denote the event that $\mathcal{A}$ outputs β' such that $\beta' = \beta$ in Game i.

Game 0. This is the standard IND-sID-CCA game. By definition we have

$$\Pr[W_0] = \frac{1}{2} + \mathsf{AdvCCA}^{\mathcal{A}}_{\mathsf{KEM}}(\kappa)$$

Game 1. Let E_{01} be the event that the adversary issues a decapsulation query $\langle I^*, C_1', C_2', C_3' \rangle$ with $C_1' = C_1^*$ in Phase 1. Note that the probability that the adversary submits a decapsulation query such that $C_1' = C_1^*$ before seeing the challenge ciphertext is bounded by Q_d/p, where Q_d is the number of decapsulation queries issued by $\mathcal{A}$. Since $Q_d = \mathsf{poly}(\kappa)$, we have $\Pr[E_{01}] \leq Q_d/p \leq \mathsf{negl}(\kappa)$. We define Game 1 exactly the same as Game 0 except assuming that E_{01} never occurs in Game 1. It follows that

$$|\Pr[W_1] - \Pr[W_0]| \leq \mathsf{negl}(\kappa)$$

Moreover, we remark that in Phase 2 a decapsulation query $\langle I^*, C_1', C_2', C_3' \rangle$ will be rejected if $C_1' = C_1^*$. Since if $C_2' \neq C_2^*$ or $C_3' \neq C_3^*$, the decapsulation query will be rejected for the inconsistency of the ciphertext. If $C_2' = C_2^*$ and $C_3' = C_3^*$, it will be rejected by definition of $\mathsf{IND\text{-}sID\text{-}CCA}$ game.

Game 2. Let E_{12} be the event that the adversary issues a decapsulation query $\langle I^*, C_1', C_2', C_3' \rangle$ with $C_1' \neq C_1^*$ and $\mathsf{TCR}(C_1') = \mathsf{TCR}(C_1^*)$. By the target collision resistance of TCR, we have $\Pr[E_{12}] \leq \mathsf{negl}(\kappa)$. We define Game 2 exactly the same as Game 1 except assuming that E_{12} never occurs in Game 2. It follows that

$$|\Pr[W_2] - \Pr[W_1]| \leq \mathsf{negl}(\kappa)$$

Game 3. We define Game 3 like Game 2, except that we sample $K_0^* \xleftarrow{R} \{0,1\}^{n\nu}$ uniformly random. Note that both K_0^* and K_1^* are chosen uniformly random, thus we have

$$\Pr[W_3] = \frac{1}{2}$$

We claim that $|\Pr[W_3] - \Pr[W_2]| \leq \mathsf{negl}(\kappa)$ under the CBDH assumption. We prove this by a hybrid argument. To this end, we define a sequence of hybrid games $H_0, \ldots, H_n$, such that H_0 equals Game 2 and H_n equals Game 3. Then we argue that hybrid H_i is indistinguishable from hybrid H_{i-1} for $i \in \{1, \ldots, n\}$ under the CBDH assumption. The claim follows, since $n = n(\kappa)$ is a polynomial. We define H_0 exactly like Game 2. Then, for i from 1 to n, in hybrid H_i we set the first $i\nu$ bits of K^* to independent random bits, and proceed otherwise exactly like in hybrid H_{i-1}. Thus, hybrid H_n proceeds exactly like Game 3. Let E_i denote the event that $\mathcal{A}$ outputs β' such that $\beta' = \beta$ in H_i. Suppose that

$$|\Pr[E_0] - \Pr[E_n]| = 1/\mathsf{poly}'(\kappa) \tag{10}$$

that is, the success probability of $\mathcal{A}$ in H_0 is not negligible close to the success probability in H_n. Note that then there must exist an index i such that $|\Pr[E_{i-1}] - \Pr[E_i]| = 1/\mathsf{poly}(\kappa)$ (since if $|\Pr[E_{i-1}] - \Pr[E_i]| \leq \mathsf{negl}(\kappa)$ for all i, then we should have $|\Pr[E_0] - \Pr[E_n]| \leq \mathsf{negl}(\kappa)$).

Suppose that there exists an algorithm $\mathcal{A}$ for which Equation (10) holds. Then we can construct an adversary $\mathcal{B}$ distinguishing the distributions Δ_{bdh} and Δ_{rand}, which by Lemma 2.3 is sufficient to prove security under the CBDH assumption in $\mathbb{G}$. Adversary $\mathcal{B}$ receives a challenge $D = (g, A, B, C, L, R)$ as input, guesses an index $\ell \in [n]$, which with probability at least $1/n$ that $|\Pr[E_{\ell-1}] - \Pr[E_\ell]| = 1/\mathsf{poly}(\kappa)$, and proceeds as follows:

Initialization. $\mathcal{A}$ first outputs an identity $I^* \in \mathbb{Z}_p$ that it intends to attack.

Setup. $\mathcal{B}$ picks $d \xleftarrow{R} \mathbb{Z}_p$, and then sets $X = A = g^a$, $X' = X^{-t^*} g^d$, $Y_\ell = B = g^b$, where $t^* = \mathsf{TCR}(C)$. For $i \in [n] \backslash \{\ell\}$, $\mathcal{B}$ picks $y_j \xleftarrow{R} \mathbb{Z}_p$ and sets $Y_i = g^{y_j}$; picks $z \xleftarrow{R} \mathbb{Z}_p$ and defines $h = X^{-I^*} g^z$. It gives $\mathcal{A}$ the public parameters $mpk = (g, h, X, X', Y_1, \ldots, Y_n, F)$. The corresponding msk, which is unknown to $\mathcal{B}$ is a. The function F is essentially of the form

$$F(x) = X^x h = X^{x - I^*} g^z$$

Phase 1 - Private Key Queries. $\mathcal{A}$ issues up to Q_e private key queries with the only restriction that $\langle I \rangle \neq \langle I^* \rangle$. To respond to a private query for identity $I \in \mathbb{Z}_p$, $\mathcal{B}$ generates $sk = (sk_1, \ldots, sk_n)$ as follows: for sk_ℓ algorithm $\mathcal{B}$ picks $s_\ell \xleftarrow{R} \mathbb{Z}_p$ and sets

$$sk_{\ell,1} = Y_\ell^{\frac{-z}{I-I^*}} F(I)^{s_\ell}, \quad sk_{\ell,2} = g^{s_\ell} Y_\ell^{\frac{-1}{I-I^*}}$$

for sk_i where $i \in [n] \backslash \{\ell\}$, $\mathcal{B}$ picks a random integer $s_i \in \mathbb{Z}_p$ and sets

$$sk_{i,1} = X^{y_i} F(I)^{s_i} = Y_i^a F(I)^{s_i}, \quad sk_{i,2} = g^{s_i}$$

Let $\widetilde{s_\ell} = s_\ell - b/(I - I^*)$. It is easy to see that sk is a valid random private key for I since

$$\begin{aligned} sk_{\ell,1} &= Y_\ell^{\frac{-z}{I-I^*}} (X^{I-I^*} g^z)^{s_\ell} = Y_\ell^a (X^{I-I^*} g^z)^{s_\ell - \frac{b}{I-I^*}} = Y_\ell^a F(I)^{\widetilde{s_\ell}} \\ sk_{\ell,2} &= g^{s_\ell} Y_\ell^{\frac{1}{I-I^*}} = g^{\widetilde{s_\ell}} \end{aligned}$$

where s_ℓ, $\widetilde{s_\ell}$ are uniform in $\mathbb{Z}_p$. This matches the definition for a private key for I. Hence, sk is a valid private key for I.

Phase 1 - Decapsulation Queries. Upon $\mathcal{A}$ issuing a decaptulation query $\langle I, C_1, C_2, C_3 \rangle$, $\mathcal{B}$ responds as follows. If $I \neq I^*$, $\mathcal{B}$ uses the corresponding private key to handle it. Otherwise, $\mathcal{B}$ computes $t = \mathsf{TCR}(C_1)$ and tests the consistency of the ciphertext by checking

$$e(C_1, X^t X') \stackrel{?}{=} e(g, C_2) \ \wedge \ e(C_1, F(I)) \stackrel{?}{=} e(g, C_3)$$

If the equality holds, $\mathcal{B}$ sets $K = (K_1, \ldots, K_n)$ as $K_i = f_{\mathrm{gl}}(e(X, C_1)^{y_i}, R)$ for $i \in [n] \backslash \{\ell\}$ and $K_\ell = f_{\mathrm{gl}}(e(\widetilde{X}, Y_\ell), R)$, where $\widetilde{X} := (C_2/C_1^d)^{1/(t-t^*)} = (X^{r(t-t^*)} g^{rd} / g^{rd})^{1/(t-t^*)} = X^r = \mathrm{dh}(X, C_1)$. By Game 2 we know that when $I = I^*$, if $C_1 \neq C_1^*$ then we have $t \neq t^*$. Therefore $\mathcal{B}$ can answer all decapsulation queries issued by $\mathcal{A}$ correctly.

Challenge. $\mathcal{B}$ sets $C_1^* = C$ (which implicitly assigns $r = c$), $C_2^* = C^d$, and $C_3^* = C^z$. The challenge ciphertext is $C^* = (C_1^*, C_2^*, C_3^*)$. Note that this is a consistent ciphertext since we have $(X^{t^*} X')^r = (g^d)^r = C^d$ and $F(I^*)^r = (g^z)^r = C^z$. Then $\mathcal{B}$ samples $i - 1$ uniformly random groups of ν bits $K_1^*, \ldots, K_{\ell-1}^*$, sets $K_\ell^* = L$, $K_i^* = f_{\mathrm{gl}}(e(X, C_1^*)^{y_i}, R)$ for i from $\ell + 1$ to n. $\mathcal{B}$ samples $U^* \in \{0,1\}^{n\nu}$ uniformly at random, and picks a random bit $\beta \in \{0,1\}$. If $\beta = 1$, it gives $\mathcal{A}$ the challenge (C^*, K^*). Otherwise it gives $\mathcal{A}$ the challenge (C^*, U^*).

Phase 2. In Phase 2, all the queries are responded in the same way as in Phase 1 except the decapsulation query $\langle I^*, C^* \rangle$ will be rejected.

This finishes the description of simulation. If $D \in \Delta_{\mathrm{bdh}}$ we have $K_\ell^* = f_{\mathrm{gl}}(\mathrm{bdh}(A, B, C), R)$, $\mathcal{A}$'s view is identical to $H_{\ell-1}$. If $D \in \Delta_{\mathrm{rand}}$, $\mathcal{A}$'s view is identical to H_ℓ. Thus $\mathcal{B}$ can use $\mathcal{A}$ to distinguish $D \in \Delta_{\mathrm{bdh}}$ from $D \in \Delta_{\mathrm{rand}}$. According to Lemma 2.3, $\mathcal{B}$ further implies a PPT algorithm which can break the CBDH problem, which contradicts to the CBDH assumption. □

D The proof of Generalized Scheme 1

Proof. We proceed in a sequence of games. We write $C^* = (C_1^*, \ldots, C_{n_2}^*)$ to denote the challenge ciphertext with the corresponding key K^* of I^*, denote with U^* the random key chosen by the IND-sID-CCA experiment, and set $t^* = \mathsf{TCR}(C_{1,1}^*, \ldots, C_{n_2,1}^*)$. We start with a game where the challenger proceeds as the standard IND-sID-CCA game (i.e., K^* is a real key and U^* is a random key), and end up with a game where both K^* and U^* are chosen uniformly random. Then we show that all games are computationally indistinguishable under the CBDH assumption. Let W_i denote the event that $\mathcal{A}$ outputs β' such that $\beta' = \beta$ in Game i.

Game 0. This is the standard IND-sID-CCA game. By definition we have

$$\Pr[W_0] = \frac{1}{2} + \mathsf{AdvCCA}^{\mathcal{A}}_{\mathsf{KEM}}(\kappa)$$

Game 1, Game 2, and Game 3 are defined in the same way as in the proof of Scheme 2. It is easy to verify that $|\Pr[W_1] - \Pr[W_0]| \leq \mathsf{negl}(\kappa)$, $|\Pr[W_2] - \Pr[W_1]| \leq \mathsf{negl}(\kappa)$, and $\Pr[W_3] = 1/2$. We claim that $|\Pr[W_3] - \Pr[W_2]| \leq \mathsf{negl}(\kappa)$ under the CBDH assumption. We prove this by a hybrid argument. To this end, we define a sequence of hybrid games $H_0, \ldots, H_n$, such that H_0 equals Game 2 and H_n equals Game 3. Then we argue that hybrid H_i is indistinguishable from hybrid H_{i-1} for $i \in \{1, \ldots, n\}$ under the CBDH assumption. The claim follows, since $n = n(\kappa)$ is a polynomial. We define H_0 exactly like Game 2. Then, for i from 1 to n, in hybrid H_i we set the first $i\nu$ bits of K^* to independent random bits, and proceed otherwise exactly like in hybrid H_{i-1}. Thus, hybrid H_n proceeds exactly like Game 3. Let E_i denote the event that $\mathcal{A}$ outputs β' such that $\beta' = \beta$ in H_i. Suppose that

$$|\Pr[E_0] - \Pr[E_n]| = 1/\mathsf{poly}'(\kappa) \tag{11}$$

that is, the success probability of $\mathcal{A}$ in H_0 is not negligible close to the success probability in H_n. Note that then there must exist an index ℓ such that $|\Pr[E_{i-1}] - \Pr[E_i]| = 1/\mathsf{poly}(\kappa)$ (since if $|\Pr[E_{i-1}] - \Pr[E_i]| \leq \mathsf{negl}(\kappa)$ for all i, then we should have $|\Pr[E_0] - \Pr[E_n]| \leq \mathsf{negl}(\kappa)$).

Suppose that there exists an algorithm $\mathcal{A}$ for which Equation (11) holds. Then we can construct an adversary $\mathcal{B}$ distinguishing the distributions Δ_{bdh} and Δ_{rand}, which by Lemma 2.3 is sufficient to prove security under the CBDH assumption in $\mathbb{G}$. Adversary $\mathcal{B}$ receives a challenge $D = (g, A, B, C, L, R)$ as input, guesses an index $\ell \in [n]$, which with probability at least $1/n$ such that $|\Pr[E_{\ell-1}] - \Pr[E_\ell]| = 1/\mathsf{poly}(\kappa)$. Let $(\bar{i}, \bar{j})$ be the unique tuple that satisfies $(\bar{i}-1) \times n_1 + \bar{j} = \ell$, $\mathcal{B}$ proceeds as follows:

Initialization. $\mathcal{A}$ first outputs an identity $I^* \in \mathbb{Z}_p$ that it intends to attack.

Setup. $\mathcal{B}$ first picks $r_j \xleftarrow{R} \mathbb{Z}_p$ for $j \in [n_2] \backslash \bar{j}$, then sets $t^* = \mathsf{TCR}(g^{r_1}, \ldots, g^{r_{\bar{j}-1}}, C, g^{r_{\bar{j}+1}}, \ldots, g^{r_{n_2}})$. $\mathcal{B}$ then picks $d \xleftarrow{R} \mathbb{Z}_p$, and sets $X = A = g^a$, $X' = X^{-t^*} g^d$, $Y_{\bar{i}} = B = g^b$; picks $y_i \xleftarrow{R} \mathbb{Z}_p$ and sets $Y_i = g^{y_i}$ for $i \in [n_1] \backslash \bar{i}$. It gives $\mathcal{A}$ the system public parameters $mpk = (g, h, X, X', Y_1, \ldots, Y_{n_2}, F)$. Note that the corresponding msk, which is unknown to $\mathcal{B}$ is a.

Phase 1 - Private Key Queries. $\mathcal{A}$ issues up to Q_e private key queries with the only restriction that $\langle I \rangle \neq \langle I^* \rangle$. To respond to the query of $I \in \mathbb{Z}_p$, for $sk_{\bar{i}}$ algorithm $\mathcal{B}$ picks $s_{\bar{i}} \xleftarrow{R} \mathbb{Z}_p$ and sets

$$sk_{\bar{i},1} = Y_{\bar{i}}^{\frac{-z}{I-I^*}} F(I)^{s_{\bar{i}}}, \quad sk_{\bar{i},2} = g^{s_{\bar{i}}} Y_{\bar{i}}^{\frac{-1}{I-I^*}}$$

for sk_i where $i \in [n_1] \backslash \{\bar{i}\}$, $\mathcal{B}$ picks a random $s_i \in \mathbb{Z}_p$ and sets

$$sk_{i,1} = X^{y_i} F(I)^{s_i} = Y_i^a F(I)^{s_i} \quad sk_{i,2} = g^{s_i}$$

Let $\widetilde{s}_{\bar{i}} = s_{\bar{i}} - b/(I - I^*)$. It is easy to see that sk is a valid random private key for I since

$$\begin{aligned} sk_{\bar{i},1} &= Y_{\bar{i}}^{\frac{-z}{I-I^*}} (X^{I-I^*} g^z)^{s_{\bar{i}}} = Y_{\bar{i}}^a (X^{I-I^*} g^z)^{s_{\bar{i}} - \frac{b}{I-I^*}} = Y_{\bar{i}}^a F(I)^{\widetilde{s}_{\bar{i}}} \\ sk_{\bar{i},2} &= g^{s_{\bar{i}}} Y_{\bar{i}}^{\frac{1}{I-I^*}} = g^{\widetilde{s}_{\bar{i}}} \end{aligned}$$

where $s_{\bar{i}}$ and $\widetilde{s}_{\bar{i}}$ are uniform distributed in $\mathbb{Z}_p$. This matches the definition of a private key for I. Hence, sk is a valid private key for I.

Phase 1 - Decapsulation Queries. Upon $\mathcal{A}$ issuing a decaptulation query $\langle I, C_1, \ldots, C_{n_2}\rangle$, $\mathcal{B}$ responds as follows. If $I \neq I^*$, $\mathcal{B}$ uses the corresponding private key to handle it. Otherwise, $\mathcal{B}$ computes $t = \mathsf{TCR}(C_{1,1}, \ldots, C_{n_2,1})$ and then tests the consistency of the ciphertext by checking

$$e(C_{j,1}, X^t X') \stackrel{?}{=} e(g, C_{j,2}) \ \wedge \ e(C_{j,1}, F(I)) \stackrel{?}{=} e(g, C_{j,3})$$

If the equality holds for all $1 \leq j \leq n_2$, then $\mathcal{B}$ computes $K = (K_1, \ldots, K_n)$ as follows. Suppose $e = (i-1) \times n_1 + j$,

1. If $i \neq \bar{i}$, set $K_e = f_{\mathrm{gl}}(e(X, C_j)^{y_i}, R)$.
2. If $i = \bar{i}$, compute $\widetilde{X_j} := (C_{j,2}/C_{j,1}^d)^{1/(t-t^*)} = (X^{r_j(t-t^*)} g^{r_j d}/g^{r_j d})^{1/(t-t^*)} = X^{r_j} = \mathrm{dh}(X, C_{j,1})$, set $K_e = f_{\mathrm{gl}}(e(\widetilde{X_j}, Y_{\bar{i}}), R)$.

By the definition of Game 2 we know that when $I = I^*$, if $C_{j,1} \neq C^*_{j,1}$ for some $j \in [n_2]$ then $t \neq t^*$. Therefore $\mathcal{B}$ can answer all decapsulation queries issued by $\mathcal{A}$ correctly.
Challenge. To generate the challenge ciphertext $C^* = (C^*_1, \ldots, C^*_{n_2})$, for $j = [n_2]\backslash\bar{j}$, $\mathcal{B}$ sets $C^*_j = (C^*_{j,1}, C^*_{j,2}, C^*_{j,3}) = (g^{r_j}, (X^{t^*}X')^{r_j}, F(I^*)^{r_j})$; for $C^*_{\bar{j}} = (C^*_{\bar{j},1}, C^*_{\bar{j},2}, C^*_{\bar{j},3})$, $\mathcal{B}$ sets $C^*_{\bar{j},1} = C$ (which implicitly assigns $r_{\bar{j}} = c$), $C^*_{\bar{j},2} = C^d$, and $C^*_{\bar{j},3} = C^z$. Note that this is a consistent ciphertext since we have $(X^{t^*}X')^{r_{\bar{j}}} = (g^d)^{r_{\bar{j}}} = C^d$ and $F(I^*)^{r_{\bar{j}}} = (g^z)^{r_{\bar{j}}} = C^z$. Then $\mathcal{B}$ samples $\ell - 1$ uniformly random groups of ν bits $K^*_1, \ldots, K^*_{\ell-1}$, sets $K^*_\ell = L$. For $\ell \leq e \leq n$, $\mathcal{B}$ generates K_e in a similar way as it did when answering decapsulation queries, that is, suppose $e = (i-1) \times n_1 + j$, if $i \neq \bar{i}$, set $K_e = f_{\mathrm{gl}}(e(X, C_j)^{y_i}, R)$; if $j \neq \bar{j}$, set $K_e = f_{\mathrm{gl}}(e(X, Y_i)^{r_j}, R)$. $\mathcal{B}$ samples $U^* \in \{0,1\}^{n\nu}$ uniformly at random, then picks a random bit $\beta \in \{0,1\}$. If $\beta = 1$, it gives $\mathcal{A}$ the challenge (C^*, K^*). Otherwise it gives $\mathcal{A}$ the challenge (C^*, U^*).
Phase 2. In Phase 2, all the queries are responded in the same way as in Phase 1 except the decapsulation query $\langle I^*, C^*\rangle$ will be rejected.

This completes the description of simulation. If $D \in \Delta_{\mathrm{bdh}}$ we have $K^*_\ell = f_{\mathrm{gl}}(\mathrm{bdh}(A, B, C), R)$, $\mathcal{A}$'s view when interacting with $\mathcal{B}$ is identical to $H_{\ell-1}$. If $D \in \Delta_{\mathrm{rand}}$, $\mathcal{A}$'s view is identical to H_ℓ. Thus $\mathcal{B}$ can use $\mathcal{A}$ to distinguish $D \in \Delta_{\mathrm{bdh}}$ from $D \in \Delta_{\mathrm{rand}}$. According to Lemma 2.3, $\mathcal{B}$ further implies a PPT algorithm which can break the CBDH problem, which contradicts to the CBDH assumption. □