this is not the case: it turns out that a slightly stronger assumption than the CDH assumption is both necessary and sufficient to prove the security of $\mathcal{E}_{\text{EG}}$.

Recall the basic ElGamal encryption scheme, $\mathcal{E}_{\text{EG}} = (G, E, D)$, introduced in Section 11.5. It is defined in terms of a cyclic group $\mathbb{G}$ of prime order q generated by $g \in \mathbb{G}$, a symmetric cipher $\mathcal{E}_{\text{s}} = (E_{\text{s}}, D_{\text{s}})$, defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$, and a hash function $H : \mathbb{G}^2 \to \mathcal{K}$. The message space of $\mathcal{E}_{\text{EG}}$ is $\mathcal{M}$ and the ciphertext space is $\mathbb{G} \times \mathcal{C}$. Public keys are of the form $u \in \mathbb{G}$ and secret keys are of the form $\alpha \in \mathbb{Z}_q$. The algorithms G, E, and D are defined as follows:

$$
\begin{aligned}
G() \quad &:= \quad \alpha \xleftarrow{\text{R}} \mathbb{Z}_q, \;\; u \leftarrow g^{\alpha}, \;\; pk \leftarrow u, \;\; sk \leftarrow \alpha \\
&\qquad \text{output } (pk, sk); \\
E(u, m) \quad &:= \quad \beta \xleftarrow{\text{R}} \mathbb{Z}_q, \;\; v \leftarrow g^{\beta}, \;\; w \leftarrow u^{\beta}, \;\; k \leftarrow H(v, w), \;\; c \xleftarrow{\text{R}} E_{\text{s}}(k, m) \\
&\qquad \text{output } (v, c); \\
D(\alpha, \; (v, c)\;) \quad &:= \quad w \leftarrow v^{\alpha}, \;\; k \leftarrow H(v, w), \;\; m \leftarrow D_{\text{s}}(k, c) \\
&\qquad \text{output } m.
\end{aligned}
$$

To see why the CDH assumption by itself is not sufficient to establish the security of $\mathcal{E}_{\text{EG}}$ against chosen ciphertext attack, suppose the public key is $u = g^{\alpha}$. Now, suppose an adversary selects group elements $\hat{v}$ and $\hat{w}$ in some arbitrary way, and computes $\hat{k} \leftarrow H(\hat{v}, \hat{w})$ and $\hat{c} \xleftarrow{\text{R}} E_{\text{s}}(\hat{k}, \hat{m})$ for some arbitrary message $\hat{m}$. Further, suppose the adversary can obtain the decryption m^* of the ciphertext $(\hat{v}, \hat{c})$. Now, it is very likely that $\hat{m} = m^*$ if and only if $\hat{w} = \hat{v}^{\alpha}$, or in other words, if and only if $(u, \hat{v}, \hat{w})$ is a DH-triple. Thus, in the chosen ciphertext attack game, decryption queries can be effectively used by the adversary to answer questions of the form "is $(u, \hat{v}, \hat{w})$ a DH-triple?" for group elements $\hat{v}$ and $\hat{w}$ of the adversary's choosing. In general, the adversary would not be able to efficiently answer such questions on his own (this is the DDH assumption), and so these decryption queries may potentially leak some information about the secret key α. Based on the current state of our knowledge, this leakage does not seem to compromise the security of the scheme; however, we do need to state this as an explicit assumption.

Intuitively, the **interactive CDH assumption** states that given a random instance (g^{α}, g^{β}) of the DH problem, it is hard to compute $g^{\alpha\beta}$, even when given access to a "DH-decision oracle" that recognizes DH-triples of the form $(g^{\alpha}, \cdot, \cdot)$. More formally, this assumption is defined in terms of the following attack game.

Attack Game 12.3 (Interactive Computational Diffie-Hellman). Let $\mathbb{G}$ be a cyclic group of prime order q generated by $g \in \mathbb{G}$. For a given adversary $\mathcal{A}$, the attack game runs as follows.

- The challenger computes

$$\alpha, \beta \xleftarrow{\text{R}} \mathbb{Z}_q, \;\; u \leftarrow g^{\alpha}, \;\; v \leftarrow g^{\beta}, \;\; w \leftarrow g^{\alpha\beta}$$

  and gives (u, v) to the adversary.

- The adversary makes a sequence of *DH-decision oracle queries* to the challenger. Each query is of the form $(\tilde{v}, \tilde{w}) \in \mathbb{G}^2$. Upon receiving such a query, the challenger tests if $\tilde{v}^{\alpha} = \tilde{w}$; if so, he sends "yes" to the adversary, and otherwise, sends "no" to the adversary.

- Finally, the adversary outputs some $\hat{w} \in \mathbb{G}$.

We define $\mathcal{A}$'s **advantage in solving the interactive computational Diffie-Hellman problem**, denoted $\text{ICDH}\mathsf{adv}[\mathcal{A}, \mathbb{G}]$, as the probability that $\hat{w} = w$. $\Box$