

Homomorphic Encryption Scheme \mathcal{E}

- ▶ $\mathcal{E} = (G, E, D)$ public-key encryption scheme
- ▶ three **groups**: plaintexts \mathcal{P} , ciphertexts $\bar{\mathcal{C}}$
 subgroup of all encryptions $\mathcal{C} := \{E_{pk}(m) \mid m \in \mathcal{P}\} \leq \bar{\mathcal{C}}$
- ▶ restricted decryption $D_{sk}|_{\mathcal{C}}$ is a group epimorphism

We can formulate an abstract *subgroup membership problem* (SMP) for $(\mathcal{C}, \mathcal{C}_0)$ whose hardness is **equivalent** to the IND-CPA security of \mathcal{E} (where $\mathcal{C}_0 := \{E_{pk}(0)\}$)!

No such scheme can be secure in terms of IND-CCA2!

Therefore, IND-CCA1 is the **strongest** security notion for homomorphic schemes.

Homomorphic Encryption Scheme \mathcal{E}

- ▶ $\mathcal{E} = (G, E, D)$ public-key encryption scheme
- ▶ three **groups**: plaintexts \mathcal{P} , ciphertexts $\bar{\mathcal{C}}$
 subgroup of all encryptions $\mathcal{C} := \{E_{pk}(m) \mid m \in \mathcal{P}\} \leq \bar{\mathcal{C}}$
- ▶ restricted decryption $D_{sk}|_{\mathcal{C}}$ is a group epimorphism

We can formulate an abstract *subgroup membership problem* (SMP) for $(\mathcal{C}, \mathcal{C}_0)$ whose hardness is **equivalent** to the IND-CPA security of \mathcal{E} (where $\mathcal{C}_0 := \{E_{pk}(0)\}$)!

No such scheme can be secure in terms of IND-CCA2!

Therefore, IND-CCA1 is the **strongest** security notion for homomorphic schemes.

Homomorphic Encryption Scheme \mathcal{E}

- ▶ $\mathcal{E} = (G, E, D)$ public-key encryption scheme
- ▶ three **groups**: plaintexts \mathcal{P} , ciphertexts $\bar{\mathcal{C}}$
subgroup of all encryptions $\mathcal{C} := \{E_{pk}(m) \mid m \in \mathcal{P}\} \leq \bar{\mathcal{C}}$
- ▶ restricted decryption $D_{sk}|_{\mathcal{C}}$ is a group epimorphism

We consider the following large **subclass**:

- ▶ sk contains an efficient *decision function* $\delta : \bar{\mathcal{C}} \rightarrow \{0, 1\}$
with $\delta(c) = 1 \iff c \in \mathcal{C}$
- ▶ decryption on $\bar{\mathcal{C}} \setminus \mathcal{C}$ returns the symbol \perp .

Almost all currently known homomorphic schemes fall into this subclass, e.g. ElGamal, Paillier, Goldwasser-Micali, Damgård's ElGamal ...

Homomorphic Encryption Scheme \mathcal{E}

- ▶ $\mathcal{E} = (G, E, D)$ public-key encryption scheme
- ▶ three **groups**: plaintexts \mathcal{P} , ciphertexts $\bar{\mathcal{C}}$
subgroup of all encryptions $\mathcal{C} := \{E_{pk}(m) \mid m \in \mathcal{P}\} \leq \bar{\mathcal{C}}$
- ▶ restricted decryption $D_{sk}|_{\mathcal{C}}$ is a group epimorphism

We consider the following large **subclass**:

- ▶ sk contains an efficient *decision function* $\delta : \bar{\mathcal{C}} \rightarrow \{0, 1\}$
with $\delta(c) = 1 \iff c \in \mathcal{C}$
- ▶ decryption on $\bar{\mathcal{C}} \setminus \mathcal{C}$ returns the symbol \perp .

Almost all currently known homomorphic schemes fall into this subclass, e.g. ElGamal, Paillier, Goldwasser-Micali, Damgård's ElGamal ...

