Crypto refresher

What's a cryptosystem

- A **cryptosystem** is a tuple Π with key, plaintext and ciphertext spaces $\mathscr{K}, \mathscr{P}, \mathscr{C}$

$$\Pi = \begin{cases} Gen : 1^n \to \mathscr{K} \\ Enc : \mathscr{K} \times \mathscr{P} \to \mathscr{C} \\ Dec : \mathscr{K} \times \mathscr{C} \to \mathscr{P} \end{cases}$$

- It is said to be **exact** (resp. **approximate**) if $\forall s \in \mathscr{K}, m \in \mathscr{P}$

For some notion of distance

$$Dec_s(Enc_s(m)) = m \text{ or } Dec_s(Enc_s(m)) \approx m$$

- It is said to be **homomorphic** if $\forall s \in \mathscr{K}, m_0, m_1 \in \mathscr{P}$

$$Enc_s(m_0 \circ m_1) = Enc_s(m_0) \circ Enc_s(m_1)$$

Crypto refresher

What's a cryptosystem

- A **cryptosystem** is a tuple Π with key, plaintext and ciphertext spaces $\mathcal{K}, \mathcal{P}, \mathcal{C}$

$$\Pi = \begin{cases} Gen : 1^n \to \mathcal{K} \\ Enc : \mathcal{K} \times \mathcal{P} \to \mathcal{C} \\ Dec : \mathcal{K} \times \mathcal{C} \to \mathcal{P} \end{cases}$$

- It is said to be **exact** (resp. **approximate**) if $\forall s \in \mathcal{K}, m \in \mathcal{P}$

$$Dec_s(Enc_s(m)) = m \text{ or } Dec_s(Enc_s(m)) \approx m$$

- It is said to be **homomorphic** if $\forall s \in \mathcal{K}, m_0, m_1 \in \mathcal{P}$

$$Enc_s(m_0 \circ m_1) = Enc_s(m_0) \circ Enc_s(m_1)$$

Modulo decryption