FYI

IND-CCA 1 and 2 of Homomorphic encryption

There exist "stronger" security properties than IND-CPA: Indistinguishability to chosen ciphertext.

Definition (IND-CCA1 Game)

IND-CCA1($\mathcal{A}$; b):
- $\mathsf{sk}, \mathsf{pk} \leftarrow \mathsf{KeyGen}()$
- $\mathsf{OrclDecrypt}(c) := \mathsf{Decrypt}(\mathsf{sk}, c)$
- $m_0, m_1 \leftarrow \mathcal{A}(\mathsf{pk}, \mathsf{OrclDecrypt})$
- $\mathsf{ct} \leftarrow \mathsf{Encrypt}(\mathsf{pk}, m_b)$
- $\mathsf{OrclDecrypt}(c) := \{\textbf{return } \perp\}$
- $b' \leftarrow \mathcal{A}(\mathsf{ct})$
- **return** $b' == b$

Definition (IND-CCA2 Game)

IND-CCA2($\mathcal{A}$; b):
- $\mathsf{sk}, \mathsf{pk} \leftarrow \mathsf{KeyGen}()$
- $\mathsf{OrclDecrypt}(c) := \mathsf{Decrypt}(\mathsf{sk}, c)$
- $m_0, m_1 \leftarrow \mathcal{A}(\mathsf{pk}, \mathsf{OrclDecrypt})$
- $\mathsf{ct} \leftarrow \mathsf{Encrypt}(\mathsf{pk}, m_b)$
- $\mathsf{OrclDecrypt}(c) := \{$
  - **if** $c == \mathsf{ct}$: **return** $\perp$
  - **else** : **return** $\mathsf{Decrypt}(\mathsf{sk}, c)\}$
- $b' \leftarrow \mathcal{A}(\mathsf{ct})$
- **return** $b' == b$

IND-CCA1 $\Longrightarrow$ IND-CPA
IND-CCA2 $\Longrightarrow$ IND-CCA1

As HE is **malleable** (by definition), IND-CCA2 cannot be achieved

Ex: Why?

There exist many more security models!

Definitions copied from Christian Mouchet's Course on Computing on Encrypted Data – HPI 2024