1. Security Scheme Definitions

Security schemes are normally presented as a game, and cryptographic systems are tested in these games to see if they are secure if an adversary cannot win a disporportionate amount of the time it.

1.1. IND-CCA (Indistinguishability under Chosen Ciphertext Attack).

Phase I:

- Examiner produces $(PK, SK) \leftarrow Keygen(1^\lambda)$.
- Adversary is given PK.
- Adversary computes in time $poly(\lambda)$ with access to decryption oracle $Dec(SK, \cdot)$ and outputs m_0, m_1 where $|m_0| = |m_1|$. The adversary can also store state information s and obtain this information in the next phase.

Phase II:

- Examiner chooses $b \leftarrow \{0, 1\}$ and computes $y = Enc(SK, m_b)$.
- Adversary is given access to state information s and allowed to compute in time $poly(\lambda)$. Then, he produces a guess $\hat{b}$.

If adversary's advantage, defined as $|P(\hat{b} = b) - \frac{1}{2}|$, is negligible then the encryption scheme is deemed secure.

Note: Encryption must be randomized, and random values cannot be easily observable for IND-CCA security.

1.2. IND-CCA2 (Indistinguishability under Adaptive Chosen Ciphertext Attack).

Adapativity is a stronger security claim than IND-CCA. Everything in IND-CCA2 is the same, except that in phase II, the adversary is given access to the decryption block $Dec(SK, \cdot)$ on all inputs except for y.

1.3. IND-CPA (Indistinguishability under Chosen Plaintext Attack).