Lecture 22: CCA Security
Recall: Public-Key Encryption

**Syntax:**
- \( \text{Gen}(1^n) \rightarrow (pk, sk) \)
- \( \text{Enc}(pk, m) \rightarrow c \)
- \( \text{Dec}(sk, c) \rightarrow m' \) or \( \bot \)

All algorithms are polynomial time

**Correctness:** For every \( m \), \( \text{Dec}(sk, \text{Enc}(pk, m)) = m \), where \( (pk, sk) \leftarrow \text{Gen}(1^n) \)
Definition (IND-CPA Security)

A public-key encryption scheme (Gen, Enc, Dec) is indistinguishably secure under chosen plaintext attack (IND-CPA) if for all n.u. PPT adversaries A, there exists a negligible function \( \mu(\cdot) \) s.t.:

\[
\Pr \left[ \begin{array}{l}
(p k, s k) \leftarrow \$ \text{Gen}(1^n), \\
(m_0, m_1) \leftarrow A(1^n, p k), \ : A(p k, \text{Enc}(m_b)) = b \\
b \leftarrow \$ \{0, 1\}
\end{array} \right] \leq \frac{1}{2} + \mu(n)
\]
Definition (IND-CPA Security)

A public-key encryption scheme $(\text{Gen}, \text{Enc}, \text{Dec})$ is indistinguishably secure under chosen plaintext attack (IND-CPA) if for all n.u. PPT adversaries $A$, there exists a negligible function $\mu(\cdot)$ s.t.:

$$\Pr \left[ \begin{array}{c}
    (pk, sk) \leftarrow \$ \text{Gen}(1^n), \\
    (m_0, m_1) \leftarrow A(1^n, pk), \quad : A(pk, \text{Enc}(m_b)) = b
\end{array} \right] \leq \frac{1}{2} + \mu(n)$$

\[ b \leftarrow \{0, 1\} \]

---

1. IND-CPA for one-message implies IND-CPA for multiple messages
What if an adversary finds a decryption box? Is IND-CPA security still enough?
Augment the IND-CPA security experiment
Security against Chosen-Ciphertext Attacks (CCA)

- Augment the IND-CPA security experiment
- Adversary can make decryption queries over ciphertext of its choice
Augment the IND-CPA security experiment
Adversary can make decryption queries over ciphertext of its choice
CCA-1: Decryption queries only before challenge ciphertext query
Security against Chosen-Ciphertext Attacks (CCA)

- Augment the IND-CPA security experiment
- Adversary can make decryption queries over ciphertext of its choice
  - **CCA-1**: Decryption queries only before challenge ciphertext query
  - **CCA-2**: Decryption queries before and after challenge ciphertext query
Security against Chosen-Ciphertext Attacks (CCA)

- Augment the IND-CPA security experiment
- Adversary can make decryption queries over ciphertext of its choice
  - **CCA-1**: Decryption queries only before challenge ciphertext query
  - **CCA-2**: Decryption queries before and after challenge ciphertext query
- No decryption query $c$ should be equal to challenge ciphertext $c^*$
CCA-1 Security

\textbf{Expt}_{A}^{\text{CCA}1}(b, z):

- \text{st} = z
CCA-1 Security

\[ \text{Expt}_{A}^{\text{CCA1}}(b, z): \]

- \( st = z \)
- \((pk, sk) \leftarrow \text{Gen}(1^n)\)
CCA-1 Security

\[ \text{Expt}^\text{CCA1}_A(b, z) : \]

- \( \text{st} = z \)
- \((pk, sk) \leftarrow \text{Gen}(1^n)\)
- Decryption query phase (repeated poly times):
CCA-1 Security

\[ \text{Expt}^{\text{CCA1}}_A (b, z) : \]

- \( \text{st} = z \)
- \((pk, sk) \leftarrow \text{Gen}(1^n)\)
- Decryption query phase (repeated poly times):
  - \( c \leftarrow A(pk, \text{st}) \)
CCA-1 Security

\[ \text{Expt}_{A}^{\text{CCA1}}(b, z): \]

- \( \text{st} = z \)
- \((pk, sk) \leftarrow \text{Gen}(1^n)\)
- Decryption query phase (repeated poly times):
  - \( c \leftarrow A(pk, \text{st}) \)
  - \( m \leftarrow \text{Dec}(sk, c) \)
CCA-1 Security

\[ \text{Expt}^{\text{CCA1}}_A (b, z): \]

- \( \text{st} = z \)
- \((pk, sk) \leftarrow \text{Gen}(1^n)\)
- Decryption query phase (repeated poly times):
  - \( c \leftarrow A(pk, \text{st}) \)
  - \( m \leftarrow \text{Dec}(sk, c) \)
  - \( \text{st} = (\text{st}, m) \)
CCA-1 Security

Expt_{ACA}^{CCA1}(b, z):

- st = z
- (pk, sk) ← Gen(1^n)
- Decryption query phase (repeated poly times):
  - $c \leftarrow A(pk, st)$
  - $m \leftarrow \text{Dec}(sk, c)$
  - $st = (st, m)$
- $(m_0, m_1) \leftarrow A(pk, st)$
CCA-1 Security

\[ \text{Expt}_{\mathcal{A}}^{\text{CCA}1}(b, z): \]

- \( \text{st} = z \)
- \((pk, sk) \leftarrow \text{Gen}(1^n)\)
- Decryption query phase (repeated poly times):
  - \( c \leftarrow \mathcal{A}(pk, \text{st}) \)
  - \( m \leftarrow \text{Dec}(sk, c) \)
  - \( \text{st} = (\text{st}, m) \)
- \((m_0, m_1) \leftarrow \mathcal{A}(pk, \text{st}) \)
- \( c^* \leftarrow \text{Enc}(pk, m_b) \)
CCA-1 Security

\[ \text{Expt}_{\mathcal{A}}^{\text{CCA}_1}(b, z) : \]

- \( \text{st} = z \)
- \((pk, sk) \leftarrow \text{Gen}(1^n)\)
- Decryption query phase (repeated poly times):
  - \( c \leftarrow \mathcal{A}(pk, \text{st}) \)
  - \( m \leftarrow \text{Dec}(sk, c) \)
  - \( \text{st} = (\text{st}, m) \)
- \((m_0, m_1) \leftarrow \mathcal{A}(pk, \text{st})\)
- \( c^* \leftarrow \text{Enc}(pk, m_b) \)
- Output \( b' \leftarrow \mathcal{A}(pk, c^*, \text{st}) \)
**CCA-1 Security**

\[ \text{Expt}_{\mathcal{A}}^{\text{CCA1}}(b, z): \]

- \( \text{st} = z \)
- \((pk, sk) \leftarrow \text{Gen}(1^n)\)
- Decryption query phase (repeated poly times):
  - \( c \leftarrow \mathcal{A}(pk, \text{st}) \)
  - \( m \leftarrow \text{Dec}(sk, c) \)
  - \( \text{st} = (\text{st}, m) \)
- \((m_0, m_1) \leftarrow \mathcal{A}(pk, \text{st}) \)
- \( c^* \leftarrow \text{Enc}(pk, m_b) \)
- Output \( b' \leftarrow \mathcal{A}(pk, c^*, \text{st}) \)
CCA-1 Security

$\text{Expt}_{\mathcal{A}}^{\text{CCA1}}(b, z)$:

- $\text{st} = z$
- $(pk, sk) \leftarrow \text{Gen}(1^n)$
- Decryption query phase (repeated poly times):
  - $c \leftarrow \mathcal{A}(pk, \text{st})$
  - $m \leftarrow \text{Dec}(sk, c)$
  - $\text{st} = (\text{st}, m)$
- $(m_0, m_1) \leftarrow \mathcal{A}(pk, \text{st})$
- $c^* \leftarrow \text{Enc}(pk, m_b)$
- Output $b' \leftarrow \mathcal{A}(pk, c^*, \text{st})$

Definition (IND-CCA-1 Security)

A public-key encryption scheme $(\text{Gen}, \text{Enc}, \text{Dec})$ is IND-CCA-1 secure if for all n.u. PPT adversaries $\mathcal{A}$, there exists a negligible function $\mu(\cdot)$ s.t. for all auxiliary inputs $z \in \{0, 1\}^*$:

$$\left| \Pr \left[ \text{Expt}_{\mathcal{A}}^{\text{CCA1}}(1, z) = 1 \right] - \Pr \left[ \text{Expt}_{\mathcal{A}}^{\text{CCA1}}(0, z) = 1 \right] \right| \leq \mu(n)$$
CCA-2 Security

\[ \text{Expt}_{A}^{\text{CCA}^2}(b, z): \]

- \[ \text{st} = z \]
CCA-2 Security

$\text{Expt}_A^{\text{CCA2}}(b, z)$:

- $\text{st} = z$
- $(pk, sk) \leftarrow \text{Gen}(1^n)$
CCA-2 Security

\[ \text{Expt}_A^{\text{CCA}^2}(b, z): \]

- \( st = z \)
- \( (pk, sk) \leftarrow \text{Gen}(1^n) \)
- Decryption query phase 1 (repeated poly times):
CCA-2 Security

\( \text{Expt}^{\text{CCA2}}_A (b, z) : \)

- \( st = z \)
- \( (pk, sk) \leftarrow \text{Gen}(1^n) \)
- Decryption query phase 1 (repeated poly times):
  - \( c \leftarrow A(pk, st) \)
CCA-2 Security

\textbf{Expt}_{A}^{\text{CCA}^2}(b, z):

- \text{st} = z
- (pk, sk) \leftarrow \text{Gen}(1^n)
- Decryption query phase 1 (repeated poly times):
  - c \leftarrow A(pk, \text{st})
  - m \leftarrow \text{Dec}(sk, c)
CCA-2 Security

\[ \text{Expt}_{A}^{\text{CCA2}}(b, z): \]

- \( st = z \)
- \((pk, sk) \leftarrow \text{Gen}(1^n)\)
- Decryption query phase 1 (repeated poly times):
  - \( c \leftarrow A(pk, st) \)
  - \( m \leftarrow \text{Dec}(sk, c) \)
  - \( st = (st, m) \)
CCA-2 Security

$$\text{Expt}_{A}^{\text{CCA2}}(b, z):$$

- \(st = z\)
- \((pk, sk) \leftarrow \text{Gen}(1^n)\)
- Decryption query phase 1 (repeated poly times):
  - \(c \leftarrow A(pk, st)\)
  - \(m \leftarrow \text{Dec}(sk, c)\)
  - \(st = (st, m)\)
- \((m_0, m_1) \leftarrow A(pk, st)\)
CCA-2 Security

Expt_{\mathcal{A}}^{\text{CCA2}}(b, z):

- st = z
- (pk, sk) \leftarrow \text{Gen}(1^n)
- Decryption query phase 1 (repeated poly times):
  - c \leftarrow \mathcal{A}(pk, st)
  - m \leftarrow \text{Dec}(sk, c)
  - st = (st, m)
- (m_0, m_1) \leftarrow \mathcal{A}(pk, st)
- c^* \leftarrow \text{Enc}(pk, m_b)
CCA-2 Security

\[ \text{Expt}_{\mathcal{A}}^{\text{CCA2}}(b, z): \]

- \( \text{st} = z \)
- \((pk, sk) \leftarrow \text{Gen}(1^n)\)
- Decryption query phase 1 (repeated poly times):
  - \( c \leftarrow \mathcal{A}(pk, \text{st}) \)
  - \( m \leftarrow \text{Dec}(sk, c) \)
  - \( \text{st} = (\text{st}, m) \)
- \((m_0, m_1) \leftarrow \mathcal{A}(pk, \text{st})\)
- \( c^* \leftarrow \text{Enc}(pk, m_b) \)
- Decryption query phase 2 (repeated poly times):
CCA-2 Security

$\text{Expt}^{\text{CCA}^2}_A(b, z)$:

- $st = z$
- $(pk, sk) \leftarrow \text{Gen}(1^n)$
- Decryption query phase 1 (repeated poly times):
  - $c \leftarrow A(pk, st)$
  - $m \leftarrow \text{Dec}(sk, c)$
  - $st = (st, m)$
- $(m_0, m_1) \leftarrow A(pk, st)$
- $c^* \leftarrow \text{Enc}(pk, m_b)$
- Decryption query phase 2 (repeated poly times):
  - $c \leftarrow A(pk, c^*, st)$

If $c \neq c^*$, output reject

Output $b_1$
CCA-2 Security

$\text{Expt}_A^{\text{CCA}_2}(b, z):$

- $\text{st} = z$
- $(pk, sk) \leftarrow \text{Gen}(1^n)$
- Decryption query phase 1 (repeated poly times):
  - $c \leftarrow A(pk, \text{st})$
  - $m \leftarrow \text{Dec}(sk, c)$
  - $\text{st} = (\text{st}, m)$
- $(m_0, m_1) \leftarrow A(pk, \text{st})$
- $c^* \leftarrow \text{Enc}(pk, m_b)$
- Decryption query phase 2 (repeated poly times):
  - $c \leftarrow A(pk, c^*, \text{st})$
  - If $c = c^*$, output reject
CCA-2 Security

Expt\textsubscript{\text{CCA}}^2(b, z):

- \text{st} = z
- (pk, sk) ← Gen(1^n)
- Decryption query phase 1 (repeated poly times):
  - c ← A(pk, st)
  - m ← Dec(sk, c)
  - \text{st} = (st, m)
- (m_0, m_1) ← A(pk, st)
- c\* ← Enc(pk, m_b)
- Decryption query phase 2 (repeated poly times):
  - c ← A(pk, c\*, st)
  - If c = c\*, output reject
  - m ← Dec(sk, c)
CCA-2 Security

$$\text{Expt}_A^{\text{CCA}2}(b, z):$$

- \text{st} = z
- \((pk, sk) \leftarrow \text{Gen}(1^n)\)
- Decryption query phase 1 (repeated poly times):
  - \(c \leftarrow A(pk, \text{st})\)
  - \(m \leftarrow \text{Dec}(sk, c)\)
  - \text{st} = (\text{st}, m)
- \((m_0, m_1) \leftarrow A(pk, \text{st})\)
- \(c^* \leftarrow \text{Enc}(pk, m_b)\)
- Decryption query phase 2 (repeated poly times):
  - \(c \leftarrow A(pk, c^*, \text{st})\)
  - If \(c = c^*\), output reject
  - \(m \leftarrow \text{Dec}(sk, c)\)
  - \text{st} = (\text{st}, m)\)
CCA-2 Security

$\text{Expt}_{A}^{\text{CCA}2}(b, z)$:

- $st = z$
- $(pk, sk) \leftarrow \text{Gen}(1^n)$
- Decryption query phase 1 (repeated poly times):
  - $c \leftarrow A(pk, st)$
  - $m \leftarrow \text{Dec}(sk, c)$
  - $st = (st, m)$
- $(m_0, m_1) \leftarrow A(pk, st)$
- $c^* \leftarrow \text{Enc}(pk, m_b)$
- Decryption query phase 2 (repeated poly times):
  - $c \leftarrow A(pk, c^*, st)$
  - If $c = c^*$, output reject
  - $m \leftarrow \text{Dec}(sk, c)$
  - $st = (st, m)$
- Output $b' \leftarrow A(pk, c^*, st)$
Definition (IND-CCA-2 Security)

A public-key encryption scheme \((\text{Gen}, \text{Enc}, \text{Dec})\) is IND-CCA-1 secure if for all n.u. PPT adversaries \(A\), there exists a negligible function \(\mu(\cdot)\) s.t. for all auxiliary inputs \(z \in \{0, 1\}^*\):

\[
\left| \Pr \left[ \text{Expt}_{A}^{\text{CCA2}}(1, z) = 1 \right] - \Pr \left[ \text{Expt}_{A}^{\text{CCA2}}(0, z) = 1 \right] \right| \leq \mu(n)
\]
Theorem

Assuming NIZKs in the CRS model and IND-CPA secure public-key encryption, there exists IND-CCA-1 secure public-key encryption.
Theorem

Assuming NIZKs in the CRS model and IND-CPA secure public-key encryption, there exists IND-CCA-1 secure public-key encryption.

Think: Proof?
Construction [Naor-Yung]

Let $(\text{Gen}, \text{Enc}, \text{Dec})$ be an IND-CPA encryption scheme.
Let $(K, P, V)$ be an adaptive NIZK.

Construction of $(\text{Gen}', \text{Enc}', \text{Dec}')$:
Construction [Naor-Yung]

Let \((\text{Gen}, \text{Enc}, \text{Dec})\) be an IND-CPA encryption scheme. Let \((K, P, V)\) be an adaptive NIZK.

Construction of \((\text{Gen}', \text{Enc}', \text{Dec}')\):

- \(\text{Gen}'(1^n)\): For \(i \in [2]\), compute \((pk_i, sk_i) \leftarrow \text{Gen}(1^n)\). Compute \(\sigma \leftarrow K(1^n)\). Set \(pk' = (pk_1, pk_2, \sigma), sk' = sk_1\).
Construction [Naor-Yung]

Let \((\text{Gen, Enc, Dec})\) be an IND-CPA encryption scheme.
Let \((K, P, V)\) be an adaptive NIZK.

Construction of \((\text{Gen}', \text{Enc}', \text{Dec}')\):

- \(\text{Gen}'(1^n)\): For \(i \in [2]\), compute \((pk_i, sk_i) \leftarrow \text{Gen}(1^n)\). Compute 
  \(\sigma \leftarrow K(1^n)\). Set \(pk' = (pk_1, pk_2, \sigma), sk' = sk_1\).

- \(\text{Enc}'(pk', m)\): For \(i \in [2]\), compute \(c_i \leftarrow \text{Enc}(pk_i, m; r_i)\). Compute 
  \(\pi \leftarrow P(\sigma, x, w)\) where \(x = (pk_1, pk_2, c_1, c_2)\), \(w = (m, r_1, r_2)\) and 
  \(R(x, w) = 1\) iff \(c_1\) and \(c_2\) encrypt same message \(m\).
Construction [Naor-Yung]

Let \((\text{Gen}, \text{Enc}, \text{Dec})\) be an IND-CPA encryption scheme.
Let \((K, P, V)\) be an adaptive NIZK.

Construction of \((\text{Gen}', \text{Enc}', \text{Dec}')\):

- \(\text{Gen}'(1^n)\): For \(i \in [2]\), compute \((pk_i, sk_i) \leftarrow \text{Gen}(1^n)\). Compute \(\sigma \leftarrow K(1^n)\). Set \(pk' = (pk_1, pk_2, \sigma), sk' = sk_1\).

- \(\text{Enc}'(pk', m)\): For \(i \in [2]\), compute \(c_i \leftarrow \text{Enc}(pk_i, m; r_i)\). Compute \(\pi \leftarrow P(\sigma, x, w)\) where \(x = (pk_1, pk_2, c_1, c_2), w = (m, r_1, r_2)\) and \(R(x, w) = 1\) iff \(c_1\) and \(c_2\) encrypt same message \(m\).

- \(\text{Dec}'(sk', c')\): If \(V(\sigma, \pi) = 0\), output \(\perp\). Else output \(\text{Dec}(sk_1, c_1)\).
Security (Hybrids)

- $H_0$: (Honest) Encryption of $m_0$
Security (Hybrids)

- \( H_0 \): (Honest) Encryption of \( m_0 \)
- \( H_1 \): Compute CRS \( \sigma \) in public key and proof \( \pi \) in challenge ciphertext using NIZK simulator
Security (Hybrids)

- $H_0$: (Honest) Encryption of $m_0$
- $H_1$: Compute CRS $\sigma$ in public key and proof $\pi$ in challenge ciphertext using NIZK simulator
- $H_2$: Change $c_2$ in challenge ciphertext to encryption of $m_1$
Security (Hybrids)

- $H_0$: (Honest) Encryption of $m_0$
- $H_1$: Compute CRS $\sigma$ in public key and proof $\pi$ in challenge ciphertext using NIZK simulator
- $H_2$: Change $c_2$ in challenge ciphertext to encryption of $m_1$
- $H_3$: Change decryption key $sk'$ to $sk_2$
Security (Hybrids)

- $H_0$: (Honest) Encryption of $m_0$
- $H_1$: Compute CRS $\sigma$ in public key and proof $\pi$ in challenge ciphertext using NIZK simulator
- $H_2$: Change $c_2$ in challenge ciphertext to encryption of $m_1$
- $H_3$: Change decryption key $sk'$ to $sk_2$
- $H_4$: Change $c_1$ in challenge ciphertext to encryption of $m_1$
Security (Hybrids)

- \( H_0 \): (Honest) Encryption of \( m_0 \)
- \( H_1 \): Compute CRS \( \sigma \) in public key and proof \( \pi \) in challenge ciphertext using NIZK simulator
- \( H_2 \): Change \( c_2 \) in challenge ciphertext to encryption of \( m_1 \)
- \( H_3 \): Change decryption key \( sk' \) to \( sk_2 \)
- \( H_4 \): Change \( c_1 \) in challenge ciphertext to encryption of \( m_1 \)
- \( H_5 \): Change decryption key \( sk' \) to \( sk_1 \)
Security (Hybrids)

- $H_0$: (Honest) Encryption of $m_0$
- $H_1$: Compute CRS $\sigma$ in public key and proof $\pi$ in challenge ciphertext using NIZK simulator
- $H_2$: Change $c_2$ in challenge ciphertext to encryption of $m_1$
- $H_3$: Change decryption key $sk'$ to $sk_2$
- $H_4$: Change $c_1$ in challenge ciphertext to encryption of $m_1$
- $H_5$: Change decryption key $sk'$ to $sk_1$
- $H_6$: Compute CRS $\sigma$ in public key and proof $\pi$ in challenge ciphertext honestly. This experiment is same as (honest) encryption of $m_1$. 
Indistinguishability of Hybrids

H₀ « H₁: ZK property of NIZK
H₁ « H₂: IND-CPA security of underlying PKE
H₂ « H₃: Only difference might be in the answers to decryption queries of adversary. But from soundness of NIZK, it follows that except with negligible probability, in each decryption query c₁, c₂, q, c₁ and c₂ encrypt same message. Therefore decrypting c₂ instead of c₁ does not change the answer.
H₃ « H₄: IND-CPA security of underlying PKE
H₄ « H₅: Same proof as in H₂ « H₃
H₅ « H₆: ZK property of NIZK

Combining the above, we get H₀ « H₆.
Indistinguishability of Hybrids

- $H_0 \approx H_1$: ZK property of NIZK
Indistinguishability of Hybrids

- $H_0 \approx H_1$: ZK property of NIZK
- $H_1 \approx H_2$: IND-CPA security of underlying PKE
Indistinguishability of Hybrids

- $H_0 \approx H_1$: ZK property of NIZK
- $H_1 \approx H_2$: IND-CPA security of underlying PKE
- $H_2 \approx H_3$: Only difference might be in the answers to decryption queries of adversary. But from soundness of NIZK, it follows that except with negligible probability, in each decryption query $c = (c_1, c_2)$, $c_1$ and $c_2$ encrypt same message. Therefore decrypting $c_2$ instead of $c_1$ does not change the answer.

- $H_4 \approx H_5$: IND-CPA security of underlying PKE
- $H_5 \approx H_6$: ZK property of NIZK.

Combining the above, we get $H_0 \approx H_6$. 
Indistinguishability of Hybrids

- $H_0 \approx H_1$: ZK property of NIZK
- $H_1 \approx H_2$: IND-CPA security of underlying PKE
- $H_2 \approx H_3$: Only difference might be in the answers to decryption queries of adversary. But from soundness of NIZK, it follows that except with negligible probability, in each decryption query $c = (c_1, c_2)$, $c_1$ and $c_2$ encrypt the same message. Therefore decrypting $c_2$ instead of $c_1$ does not change the answer.
- $H_3 \approx H_4$: IND-CPA security of underlying PKE

Combining the above, we get $H_0 \approx H_6$. 

Lecture 22: CCA Security
Indistinguishability of Hybrids

- $H_0 \approx H_1$: ZK property of NIZK
- $H_1 \approx H_2$: IND-CPA security of underlying PKE
- $H_2 \approx H_3$: Only difference might be in the answers to decryption queries of adversary. But from soundness of NIZK, it follows that except with negligible probability, in each decryption query $c = (c_1, c_2)$, $c_1$ and $c_2$ encrypt same message. Therefore decrypting $c_2$ instead of $c_1$ does not change the answer.
- $H_3 \approx H_4$: IND-CPA security of underlying PKE
- $H_4 \approx H_5$: Same proof as in $H_2 \approx H_3$
Indistinguishability of Hybrids

- $H_0 \approx H_1$: ZK property of NIZK
- $H_1 \approx H_2$: IND-CPA security of underlying PKE
- $H_2 \approx H_3$: Only difference might be in the answers to decryption queries of adversary. But from soundness of NIZK, it follows that except with negligible probability, in each decryption query $c = (c_1, c_2)$, $c_1$ and $c_2$ encrypt same message. Therefore decrypting $c_2$ instead of $c_1$ does not change the answer.
- $H_3 \approx H_4$: IND-CPA security of underlying PKE
- $H_4 \approx H_5$: Same proof as in $H_2 \approx H_3$
- $H_5 \approx H_6$: ZK property of NIZK
Indistinguishability of Hybrids

- $H_0 \approx H_1$: ZK property of NIZK
- $H_1 \approx H_2$: IND-CPA security of underlying PKE
- $H_2 \approx H_3$: Only difference might be in the answers to decryption queries of adversary. But from soundness of NIZK, it follows that except with negligible probability, in each decryption query $c = (c_1, c_2)$, $c_1$ and $c_2$ encrypt same message. Therefore decrypting $c_2$ instead of $c_1$ does not change the answer.
- $H_3 \approx H_4$: IND-CPA security of underlying PKE
- $H_4 \approx H_5$: Same proof as in $H_2 \approx H_3$
- $H_5 \approx H_6$: ZK property of NIZK

Combining the above, we get $H_0 \approx H_6$. 