Section 1

Definitions
Correctness

Definition 1 (encryption scheme)

A trippet of PPTM’s \((G, E, D)\) such that

1. \(G(1^n)\) outputs \((e, d) \in \{0, 1\}^* \times \{0, 1\}^*\)
2. \(E(e, m)\) outputs \(c \in \{0, 1\}^*\)
3. \(D(d, c)\) outputs \(m \in \{0, 1\}^*\)

Correctness: \(D(d, E(e, m)) = m\), for any \((e, d) \in \text{Supp}(G(1^n))\) and \(m \in \{0, 1\}^*\)

- \(e\) – encryption key, \(d\) – decryption key
- \(m\) – plaintext, \(c = E(e, m)\) – ciphertext
- \(E_e(m) \equiv E(e, m)\) and \(D_d(c) \equiv D(d, c)\),

- public/private key
What would we like to achieve?

Attempt: for any $m \in \{0, 1\}^*$:

$$(m, E_{(G(1^n)_1)}(m)) \equiv (m, U_\ell(|m|))$$

- Shannon – only possible in case $|m| \leq |G(1^n)_1|$
- Other concerns: multiple encryptions, active adversaries, ...
Semantic Security

1. Ciphertext reveals no "computation information" about the plaintext
2. Formulate via the \textit{simulation paradigm}
3. Does not hide the message \textit{length}
Definition 2 (Semantic Security — private-key model)

An encryption scheme \((G, E, D)\) is semantically secure in the private-key model, if \(\forall\) PPTM \(A, \exists\) PPTM \(A'\) s.t.:

\[\forall\ \text{poly-length dist. ensemble } M = \{M_n\}_{n \in \mathbb{N}} \text{ and poly-length functions } h, f : \{0, 1\}^* \rightarrow \{0, 1\}^*\]

\[
\left| \Pr_{m \leftarrow M_n, e \leftarrow G(1^n)} [A(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] - \Pr_{m \leftarrow M_n} [A'(1^n, 1^{|m|}, h(1^n, m)) = f(1^n, m)] \right| = \text{neg}(n)
\]

- Non uniformity is inherent.
- Public-key variant — \(A\) and \(A'\) get \(e\)
- Reflection to \(\mathcal{ZK}\)
- We sometimes omit \(1^n\) and \(1^{|m|}\)
Indistinguishability of Encryptions

- The encryption of two strings is indistinguishable
- Less intuitive than semantic security, but easier to work with

**Definition 3 (Indistinguishability of encryptions — private-key model)**

An encryption scheme \((G, E, D)\) has indistinguishable encryptions in the private-key model, if for any \(p, \ell \in \text{poly}\), \(\{x_n, y_n \in \{0, 1\}^{\ell(n)}\}_{n \in \mathbb{N}}\) and \(\{z_n \in \{0, 1\}^{p(n)}\}_{n \in \mathbb{N}}\)

\[
\{(z_n, E_e(x_n))_{e \leftarrow G(1^n)}\}_{n \in \mathbb{N}} \approx_c \{(z_n, E_e(y_n))_{e \leftarrow G(1^n)}\}_{n \in \mathbb{N}}
\]

- Non uniformity is inherent.
- Public-key variant — the ensemble contains \(e\)
Equivalence of Definitions

Theorem 4

An encryption scheme \((G, E, D)\) is semantically secure iff it has indistinguishable encryptions.

We prove the private key case
Indistinguishability  $\implies$  Semantic Security

Fix $\mathcal{M}$, $A$, $f$ and $h$, as in Definition 2.

**Algorithm 5 ($A'$)**

**Input:** $1^n, 1^{|m|}$ and $h(m)$

1. $e \leftarrow G(1^n)$
2. $c = E_e(1^{|m|})$
3. Output $A(1^n, 1^{|m|}, h(m), c)$

**Claim 6**

$A'$ is a good simulator for $A$ (according to Definition 2)

**Proof:** Let

$$
\delta(n) := \Pr_{m \leftarrow \mathcal{M}_n, e \leftarrow G(1^n)} [A(h(m), E_e(m)) = f(m)] - \Pr_{m \leftarrow \mathcal{M}_n} [A'(h(m)) = f(m)]
$$

We define an algorithm that distinguish two between two ensembles $\{x_n\}_{n \in \mathbb{N}}$ and $\{y_n\}_{n \in \mathbb{N}}$, with advantage $\delta(n)$.

Hence, the indistinguishability of $(G, E, D)$ yields that $\delta(n) \leq \text{neg}(n)$. 
The Distinguisher

Claim 7

For every \( n \in \mathbb{N} \), exists \( x_n \in \text{Supp}(\mathcal{M}_n) \) with

\[
\Pr_{e \leftarrow G(1^n)} \left[ A(h(x_n), E_e(x_n)) = f(x_n) \right] - \Pr \left[ A'(h(x_n)) = f(x_n) \right] \geq \delta(n).
\]

Proof: ?

Algorithm 8 (B)

**Input:** \( 1^n, 1^t, h', f', c \)

**Output 1 iff** \( A(1^n, 1^t, h', c) = f' \)

Let \( \{ z_n = (1^n, 1^{|x_n|}, h(x_n), f(x_n)) \}_n \in \mathbb{N} \).

\[
\Pr_{e \leftarrow G(1^n)} \left[ B(z_n, E_e(x_n)) = 1 \right] = \\
\Pr_{e \leftarrow G(1^n)} \left[ A(1^n, 1^{|x_n|}, h(x_n), E_e(x_n)) = f(x_n) \right]
\]

\[
\Pr_{e \leftarrow G(1^n)} \left[ B(z_n, E_e(1^{|x_n|})) = 1 \right] = \Pr \left[ A'(1^n, 1^{|x_n|}, h(x_n)) = f(x_n) \right]
\]

Hence,

\[
\Pr_{e \leftarrow G(1^n)} \left[ B(z_n, E_e(x_n)) = 1 \right] - \Pr_{e \leftarrow G(1^n)} \left[ B(z_n, E_e(1^{|x_n|})) = 1 \right] \geq \delta(n),
\]
Semantic Security $\implies$ Indistinguishability

For PPT $B$, $\{x_n, y_n \in \{0, 1\}^{\ell(n)} \}_{n \in \mathbb{N}}$ and $\{z_n\}_{n \in \mathbb{N}}$, let

$$\delta(n) = \Pr_{e \leftarrow G(1^n)} [B(z_n, E_e(x_n)) = 1] - \Pr_{e \leftarrow G(1^n)} [B(z_n, E_e(y_n)) = 1]$$

We define distribution $M$, functions $f, h$ and algorithm $A$ that has no $\delta(n)/4$ simulator. The semantic security of $(G, E, D)$ yields that $\delta(n) \leq \text{neg}(n)$.

Let $f(x_n) = 1$ and $f(y_n) = 0$, and let $A(w)$ output 1 if $B(w) = 1$, and a uniform bit otherwise.

**Claim 9**

$$\Pr_{e \leftarrow G(1^n), t_n \leftarrow \{x_n, y_n\}} [A(z_n, E_e(t_n)) = f(t_n)] = \frac{1}{2} + \frac{\delta(n)}{4}$$

**Proof:** Let $\alpha(n) = \Pr_{e \leftarrow G(1^n)} [B(z_n, E_e(x_n)) = 1]$.

$$\Pr_{e \leftarrow G(1^n)} [A(z_n, E_e(x_n)) = f(x_n)] = \alpha(n) + \frac{1}{2}(1 - \alpha(n)) = \frac{1}{2} + \frac{\alpha(n)}{2}$$

and

$$\Pr_{e \leftarrow G(1^n)} [A(z_n, E_e(y_n)) = f(y_n)] = \frac{1}{2} + \frac{\delta(n) - \alpha(n)}{2}$$
Semantic Security $\iff$ Indistinguishability, cont.

- Let $\mathcal{M}_n$ be $x_n$ w.p. $\frac{1}{2}$, and $y_n$ otherwise.
- Let $h(1^n, \cdot) = z_n$, and recall $f(x_n) = 1$ and $f(y_n) = 0$.

By Claim 9:

$$\Pr_{m \leftarrow \mathcal{M}_n, e \leftarrow G(1^n)} \left[ A(h(1^n, m), E_e(m)) = f(m) \right] = \frac{1}{2} + \frac{\delta(n)}{2}$$

But, for any $A'$:

$$\Pr_{m \leftarrow \mathcal{M}_n, e \leftarrow G(1^n)} \left[ A'(h(1^n, m)) = f(m) \right] \leq \frac{1}{2}$$

Hence, $\delta(n) \leq \text{neg}(n)$. 
Security Under Multiple Encryptions

Definition 10 (Indistinguishability for multiple encryptions – private-key model)

An encryption scheme \((G, E, D)\) has indistinguishable encryptions for multiple messages in the private-key model, if for any \(p, \ell, t \in \text{poly}\), \(\{x_{n,1}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)} \in \{0, 1\}^{\ell(n)}\}_{n \in \mathbb{N}}, \{z_n \in \{0, 1\}^{p(n)}\}_{n \in \mathbb{N}}, \text{PPTM } B:\)

\[
\left| \Pr_{e \leftarrow G^{(1^n)}} [B(z_n, E_e(x_{n,1}), \ldots E_e(x_{n,t(n)})) = 1] \right| - \left| \Pr_{e \leftarrow G^{(1^n)}} [B(z_n, E_e(y_{n,1}), \ldots E_e(y_{n,t(n)})) = 1] \right| = \text{neg}(n)
\]

Extensions:

- Different length messages
- Semantic security version
- Public-key variant
Theorem 11

A public-key encryption scheme has indistinguishable encryptions for multiple messages, iff it has indistinguishable encryptions for a single message.

Proof: Let \((G, E, D)\) be a public-key encryption scheme that has no indistinguishable encryptions for multiple messages, with respect to PPT \(B\), \(\{x_{n,1}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)} \in \{0, 1\}^\ell(n)\}_{n \in \mathbb{N}}, \{Z_n \in \{0, 1\}^p(n)\}_{n \in \mathbb{N}}\).

Hence, for some function \(i(n) \in [t(n)]\):

\[
\left| \Pr_{e \leftarrow G(1^n)_1} \left[ B(1^n, e, E_e(x_{n,1}), \ldots, E_e(x_{n,i-1}), E_e(y_{n,i}) \ldots, E_e(y_{n,t(n)})) = 1 \right] - \Pr_{e \leftarrow G(1^n)_1} \left[ B(1^n, e, E_e(x_{n,1}), \ldots, E_e(x_{n,i}), E_e(y_{n,i+1}) \ldots, E_e(y_{n,t(n)})) = 1 \right] \right| > \text{neg}(n).
\]

Thus, \((G, E, D)\) has no indistinguishable encryptions for single message:

Algorithm 12 (B’)

Input: \(1^n, Z_n = (i(n), x_{n,1}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)}), e, c\)
Return \(B(c, E_e(x_{n,1}), \ldots, E_e(x_{n,i-1}), c, E_e(y_{n,i+1}) \ldots, E_e(y_{n,t(n)}))\)
Multiple Encryption in the Private-Key Model

Fact 13

Assuming (non uniform) OWFs exists, then \( \exists \) encryption scheme that has private-key indistinguishable encryptions for a single messages, but **not** for multiple messages.

Proof: Let \( g: \{0, 1\}^n \mapsto \{0, 1\}^{n+1} \) be a (non-uniform) PRG, and for \( i \in \mathbb{N} \) let \( g^i \) be its "iterated extension" to output of length \( n + i \) (see Lecture 2).

Construction 14

- \( G(1^n) \): outputs \( e \leftarrow \{0, 1\}^n \)
- \( E_e(m) \): outputs \( g^{|m|}(e) \oplus m \)
- \( D_e(c) \): outputs \( g^{|c|}(e) \oplus c \)
**Claim 15**

\((G, E, D)\) has private-key indistinguishable encryptions for a single message

Proof: Assume not, and let \(B, \{x_n, y_n \in \{0, 1\}^{\ell(n)}\}_{n \in \mathbb{N}}\) and \(\{z_n \in \{0, 1\}^{p(n)}\}_{n \in \mathbb{N}}\) be the triplet that realizes it:

\[|\Pr[B(z_n, g^{\ell(n)}(U_n) \oplus x_n) = 1] - \Pr[B(z_n, g^{\ell(n)}(U_n) \oplus y_n) = 1]| > \text{neg}(n) \quad (1)\]

Hence, \(B\) yields a (non-uniform) distinguisher for \(g\). (?)

**Claim 16**

\((G, E, D)\) does not have a private-key indistinguishable encryptions for multiple messages

Proof: Take \(x_{n,1} = x_{n,2}\) and \(y_{n,1} \neq y_{n,2}\), and let \(B\) be the algorithm that on input \((c_1, c_2)\), outputs 1 iff \(c_1 = c_2\). \(\Box\)
Section 2

Constructions
Private-Key Indistinguishable Encryptions for Multiple Messages

Suffices to encrypt messages of some fixed length (here the length is \( n \)).

Let \( \mathcal{F} \) be a (non-uniform) length-preserving PRF

**Construction 17**

- **\( G(1^n) \):** output \( e \leftarrow \mathcal{F}_n \)
- **\( E_e(m) \):** choose \( r \leftarrow \{0, 1\}^n \) and output \( (r, e(r) \oplus m) \)
- **\( D_e(r, c) \):** output \( e(r) \oplus c \)

**Claim 18**

\((G, E, D)\) has private-key indistinguishable encryptions for a multiple messages

**Proof:** ?
Public-key indistinguishable encryptions for multiple messages

Let \((G_T, f, Inv)\) be a (non-uniform) TDP, and let \(b\) be hardcore predicate for it.

**Construction 19 (bit encryption)**

- \(G(1^n)\): output \((e, d) \leftarrow G_T(1^n)\)
- \(E_e(m)\): choose \(r \leftarrow \{0, 1\}^n\) and output \((y = f_e(r), c = b(r) \oplus m)\)
- \(D_d(y, c)\): output \(b(\text{Inv}_d(y)) \oplus c\)

**Claim 20**

\((G, E, D)\) has public-key indistinguishable encryptions for a multiple messages

**Proof:**

We believe that public-key encryptions schemes are “more complex" than private-key ones
Section 3

Active Adversaries
Active Adversaries

- **Chosen plaintext attack (CPA):**
  The adversary can ask for encryption and choose the messages to distinguish accordingly

- **Chosen ciphertext attack (CCA):**
  The adversary can also ask for **decryptions** of certain messages

- In the public-key settings, the adversary is also given the public key

- We focus on indistinguishability, but each of the above definitions has an equivalent semantic security variant.
**CPA Security**

Let \((G, E, D)\) be an encryption scheme. For a pair of algorithms \(A = (A_1, A_2)\), \(n \in \mathbb{N}\), \(z \in \{0, 1\}^*\) and \(b \in \{0, 1\}\), let:

**Experiment 21** \((\text{Exp}_{A,n,z}^{\text{CPA}}(b))\)

1. \((e, d) \leftarrow G(1^n)\)

2. \((m_0, m_1, s) \leftarrow A_1^{E_e(\cdot)}(1^n, z)\), where \(|m_0| = |m_1|\).

3. \(c \leftarrow E_e(m_b)\)

4. Output \(A_2^{E_e(\cdot)}(1^n, s, c)\)

**Definition 22 (private key CPA)**

\((G, E, D)\) has indistinguishable encryptions in the private-key model under CPA attack, if \(\forall \) PPT \(A_1, A_2\), and poly-bounded \(\{z_n\}_{n \in \mathbb{N}}\):

\[
| \Pr[\text{Exp}_{A,n,z_n}^{\text{CPA}}(0) = 1] - \Pr[\text{Exp}_{A,n,z_n}^{\text{CPA}}(1) = 1] | = \text{neg}(n)
\]
public-key variant.

The scheme from Construction 17 has indistinguishable encryptions in the private-key model under CPA attack (for short, private-key CPA secure)

The scheme from Construction 19 has indistinguishable encryptions in the public-key model under CPA attack (for short, public-key CPA secure)

In both cases, definitions are not equivalent (?)
CCA Security

Experiment 23 (Exp_{CCA^1}^{A,n,z}(b))

1. \((e, d) \leftarrow G(1^n)\)
2. \((m_0, m_1, s) \leftarrow A_{1}^{E_{e}(\cdot), D_{d}(\cdot)}(1^n, z)\), where \(|m_0| = |m_1|\).
3. \(c \leftarrow E_{e}(m_b)\)
4. Output \(A_{2}^{E_{e}(\cdot)}(1^n, s, c)\)

Experiment 24 (Exp_{CCA^2}^{A,n,z_n}(b))

1. \((e, d) \leftarrow G(1^n)\)
2. \((m_0, m_1, s) \leftarrow A_{1}^{E_{e}(\cdot), D_{d}(\cdot)}(1^n, z)\), where \(|m_0| = |m_1|\).
3. \(c \leftarrow E_{e}(m_b)\)
4. Output \(A_{2}^{E_{e}(\cdot), D_{d}^{-c}(\cdot)}(1^n, s, c)\)
Definition 25 (private key CCA1/CCA2)

\((G, E, D)\) has indistinguishable encryptions in the private-key model under
\(x \in \{\text{CCA1, CCA2}\}\) attack, if \(\forall\) PPT \(A_1, A_2\), and poly-bounded \(\{z_n\}_{n \in \mathbb{N}}\):

\[
| \Pr[\text{Exp}_{A_1, n, z_n}^x(0) = 1] - \Pr[\text{Exp}_{A_2, n, z_n}^x(1) = 1] | = \text{neg}(n)
\]

- The public key definition is analogous
**Private-key CCA2**
- Is the scheme from Construction 17 private-key CCA1 secure?
- CCA2 secure?

Let \((G, E, D)\) be a private-key CPA scheme, and let \((\text{Gen}_M, \text{Mac}, \text{Vrfy})\) be an existential unforgeable strong MAC.

**Construction 26**
- \(G'(1^n): \text{Output } (e \leftarrow G_E(1^n), k \leftarrow \text{Gen}_M(1^n)).^a\)
- \(E'_{e,k}(m): \text{let } c = E_e(m) \text{ and output } (c, t = \text{Mac}_k(c))\)
- \(D_{e,k}(c, t): \text{if } \text{Vrfy}_k(c, t) = 1, \text{output } D_e(c). \text{Otherwise, output } \perp\)

^aWe assume wlg. that the encryption and decryption keys are the same.

**Theorem 27**

*Construction 26 is a private-key CCA2-secure encryption scheme.*

Proof: An attacker on the CCA2-security of \((G', E', D')\) yields an attacker on the CPA security of \((G, E, D)\), or the existential unforgettablly of \((\text{Gen}_M, \text{Mac}, \text{Vrfy})\).
Public-key CCA1

Let \((G, E, D)\) be a public-key CPA scheme and let \((P, V)\) be a NIZK for \(L = \{ (c_0, c_1, pk_0, pk_1) : \exists (m, z_0, z_1) \text{ s.t. } c_0 = E_{pk_0}(m, z_0) \land c_1 = E_{pk_1}(m, z_1) \}\)

Construction 28 (The Naor-Yung Paradigm)

- **\(G'(1^n)\):**
  1. For \(i \in \{0, 1\}\): set \((sk_i, pk_i) \leftarrow G(1^n)\).
  2. Let \(r \leftarrow \{0, 1\}^\ell(n)\), and output \(pk' = (pk_0, pk_1, r)\) and \(sk' = (pk', sk_0, sk_1)\)

- **\(E'_{pk'}(m)\):**
  1. For \(i \in \{0, 1\}\): set \(c_i = E_{pk_i}(m, z_i)\), where \(z_i\) is a uniformly chosen string of the right length
  2. \(\pi \leftarrow P((c_0, c_1, pk_0, pk_1), (m, z_0, z_1), r)\)
  3. Output \((c_0, c_1, \pi)\).

- **\(D'_{sk'}(c_0, c_1, \pi)\):** If \(V((c_0, c_1, pk_0, pk_1), \pi, r) = 1\), return \(D_{sk_0}(c_0)\).
  Otherwise, return \(\bot\).
We assume for simplicity that the encryption key output by $G(1^n)$ is of length at least $n$. (?)

- $\ell$ is an arbitrary polynomial, and determines the maximum message length to encrypt using "security parameter" $n$.

Is the scheme CCA1 secure?

**Theorem 29**

*Assuming* $(P, V)$ *is adaptive secure, then Construction 28 is a public-key CCA1 secure encryption scheme.*

*Proof:* Given an attacker $A'$ for the CCA1 security of $(G', E', D')$, we use it to construct an attacker $A$ on the CPA security of $(G, E, D)$ or the adaptive security of $(P, V)$. 
Proving Thm 29

Let $S = (S_1, S_2)$ be the (adaptive) simulator for $(P, V, \mathcal{L})$

**Algorithm 30 (A)**

**Input:** $(1^n, pk)$

1. Let $j \leftarrow \{0, 1\}$, $pk_{1-j} = pk$, $(pk_j, sk_j) \leftarrow G(1^n)$ and $(r, s) \leftarrow S_1(1^n)$

2. Emulate $A'(1^n, pk' = (pk_0, pk_1, r))$:
   - On query $(c_0, c_1, \pi)$ of $A'$ to $D'$:
     - If $V((c_0, c_1, pk_0, pk_1), \pi, r) = 1$, answer $D_{sk_j}(c_j)$.
     - Otherwise, answer $\bot$.

3. Output the pair $(m_0, m_1)$ that $A'$ outputs

4. On challenge $c (~= E_{pk}(m_b))$:
   - Set $c_{1-j} = c$, $c_j = E_{pk_j}(m_a)$ for $a \leftarrow \{0, 1\}$, and $\pi \leftarrow S_2((c_0, c_1, pk_0, pk_1), r, s)$
   - Send $c' = (c_0, c_1, \pi)$ to $A'$

5. Output the value that $A'$ does
Claim 31

Assume $A'$ breaks the CCA1 security of $(G', E', D')$ w.p. $\delta(n)$, then $A$ breaks the CPA security of $(G, E, D)$ w.p. $(\delta(n) - \text{neg}(n))/2$.

The adaptive soundness and adaptive zero-knowledge of $(P, V)$, yields that

$$\Pr[A' \text{ "makes" } A(1^n) \text{ decrypt an invalid cipher}] = \text{neg}(n)$$ (2)

Assume for simplicity that the above prob is 0. Hence, in the first the emulation of $A'$ is perfect and leaks no information about $j$.

Let $A'(1^n, x, y)$ be $A'$’s output in the emulation induced by $A(1^n)$, conditioned on $a = x$ and $b = y$.

1. Since no information about $j$ has leaked, $A'(1^n, 0, 1) \equiv A'(1^n, 1, 0)$

2. The adaptive zero-knowledge of $(P, V)$ yields that

$$|\Pr[A'(1^n, 1, 1) = 1] - \Pr[A'(1^n, 0, 0) = 1]| \geq \delta(n) - \text{neg}(n)$$
Let $A(x)$ be $A$'s output on challenge $E_{pk}(m_x)$ (and security parameter $1^n$).

\[ |\Pr[A(1) = 1] - \Pr[A(0) = 1]| \]
\[ = \left| \frac{1}{2}(\Pr[A'(0, 1) = 1] + \Pr[A'(1, 1) = 1]) - \frac{1}{2}(\Pr[A'(0, 0) = 1] + \Pr[A'(1, 0) = 1]) \right| \]
\[ \geq \frac{1}{2} |\Pr[A'(1, 1) = 1] - \Pr[A'(0, 0) = 1]| - \frac{1}{2} |\Pr[A'(1, 0) = 1] - \Pr[A'(0, 1) = 1]| \]
\[ \geq (\delta(n) - \text{neg}(n))/2 - 0 \]
Is Construction 28 CCA2 secure?

**Problem:** Soundness might not hold with respect to the simulated CRS, after seeing a proof for an invalid statement

**Solution:** use simulation sound NIZK