CS 555: Cryptography

Perfectly Secret Encryption
Perfectly Secret Encryption (PSE)

The following definition of PSE implies that unbounded computing is of no use to an adversary:

\[
\Pr(M = m \mid C = c) = \Pr(M = m) \quad (1)
\]

[ Note: In all such equations, we implicitly assume a “for all” (not “there exists”) quantification. For (1), this means “for all \( m, c, \) and distributions of \( M \)” is implicit ]
Equivalent Definition (2)

- $\Pr( M = m | C = c ) = \Pr( M = m )$ \hspace{1cm} (1)
  
  $\{M=m\}$ and $\{C=c\}$ are independent \hspace{1cm} (2)

Proof that (1) and (2) are equivalent:

$\Pr(M=m | C=c) = \Pr(M=m,C=c) / \Pr(C=c)$ \hspace{1cm} (*)

(1) implies that LHS of (*) = $\Pr(M=m)$, therefore:

$\Pr(M=m) \Pr(C=c) = \Pr(M=m,C=c)$ and (2) holds

(2) implies: $\Pr(M=m,C=c) = \Pr(M=m) \Pr(C=c)$

Which, when used in (*), gives (1)
Equivalent Definition (3)

- \( \Pr( C = c \mid M = m ) = \Pr( C = c ) \) \hspace{1cm} (3)

Proof that above implies perfect secrecy:

By definition of conditional probability, we have

\[
\Pr(C=c \mid M=m) = \frac{\Pr(C=c,M=m)}{\Pr(M=m)}
\]

Using hypothesis on LHS of above gives:

\[
\Pr(C=c) = \frac{\Pr(C=c,M=m)}{\Pr(M=m)}
\]

\[
\Pr(C=c,M=m) = \Pr(C=c) \Pr(M=m)
\]

Therefore \{M=m\} and \{C=c\} are independent which is Defn. (2) of perfectly secure encryption

[ Note: Proof in other direction is easy ]
Equivalent Definition (4)

\[ \Pr( E_k(m) = c ) = \Pr( E_k(m') = c ) \]  \hspace{1cm} (4)

Proof that above implies perfect secrecy:
Both sides of the following eqn. (*) equal \( \Pr(M=m, C=c) \):

\[ \Pr(M=m \mid C=c) \Pr(C=c) = \Pr(C=c \mid M=m) \Pr(M=m) \]  \hspace{1cm} (*)

\[ \Pr(C=c) = \Pr(U_{m'} \{ C=c, M=m' \} ) \]

\[ = \sum_{m'} \Pr(C=c, M=m') \]
\[ = \sum_{m'} \Pr(C=c \mid M=m') \Pr(M=m') \]
\[ = \sum_{m'} \Pr(E_k(m')=c) \Pr(M=m') \]
\[ = \sum_{m'} \Pr(E_k(m)=c) \Pr(M=m') \]
\[ = \Pr(E_k(m)=c) \left( \sum_{m'} \Pr(M=m') \right) \]
\[ = \Pr(E_k(m)=c) \]  \hspace{1cm} which, when used in (*), gives:
Equivalent Definition (4)

\[
\Pr(M=m|C=c) \Pr(E_k(m)=c) = \Pr(C=c|M=m)\Pr(M=m)
\]

which, after replacing \(\Pr(C=c|M=m)\) with \(\Pr(E_k(m)=c)\), becomes:

\[
\Pr(M=m|C=c) \Pr(E_k(m)=c) = \Pr(E_k(m)=c) \Pr(M=m)
\]

Simplifying the above gives:

\[
\Pr(M=m|C=c) = \Pr(M=m)
\]

which is recognized as Definition (1) of perfectly secret encryption
Equivalent Definition (5)

- **Perfect indistinguishability**
- **Game played with adversary $A$:**
  - $A$ outputs a pair of distinct messages $m_0$, $m_1$
  - $A$ is given a challenge $E_k(m_b)$ where $b$ is a random bit and $k$ is a random key
  - $A$ guesses whether $b$ is 0 or 1, succeeds if the guess is correct
- **An encryption scheme is perfectly indistinguishable if, for every $A$, the probability that $A$ succeeds is $1/2$**
More formally:

The adversarial indistinguishability experiment $\text{PrivK}_{A,\Pi}^{\text{eav}}$:

1. The adversary $A$ outputs a pair of messages $m_0, m_1 \in \mathcal{M}$.
2. A key $k$ is generated using $\text{Gen}$, and a uniform bit $b \in \{0, 1\}$ is chosen. Ciphertext $c \leftarrow \text{Enc}_k(m_b)$ is computed and given to $A$. We refer to $c$ as the challenge ciphertext.
3. $A$ outputs a bit $b'$.
4. The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise. We write $\text{PrivK}_{A,\Pi}^{\text{eav}} = 1$ if the output of the experiment is 1 and in this case we say that $A$ succeeds.

Encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ with message space $\mathcal{M}$ is perfectly indistinguishable if for every adversary $A$ it holds that:

$$\Pr[\text{PrivK}_{A,\Pi}^{\text{eav}} = 1] = \frac{1}{2}$$
Proof that Perfect Indistinguishability (PI) implies Perfect Security (PS)

If PI holds and PS doesn’t, then Definition (3) must be violated for some \(m, m', c\) such that

\[
\Pr( E_k(m) = c ) > \Pr( E_k(m') = c )
\]

An \(A\) who knows that \(m\) is more likely than \(m'\) can, in the game, choose

\[
m_0 = m
\]
\[
m_1 = m'
\]

then give a response biased towards \(m_0\) that achieves a prob. of success greater than 0.5
Proof that Perfect Security implies Perfect Indistinguishability

For every choice of $m_0$ and $m_1$ made by $\mathcal{A}$ in the game, perfect secrecy implies that

$$\Pr( E_k(m_0) = c ) = \Pr( E_k(m_1) = c )$$

Therefore every response to the challenge ciphertext by $\mathcal{A}$ has probability 0.5 of being correct.
One-time pad (a.k.a. Vernam cipher)

- Encrypt message $m$ by bitwise XOR with a key $k$ that is uniformly generated:
  \[ c = m \oplus k \]
- Decryption is bitwise XOR with same $k$:
  \[ c \oplus k = m \oplus k \oplus k = m \oplus 0 = m \]
- $m$, $k$, $c$, have same number of bits, hence:
  \[ |M| = |K| = |C| \]
One-time pad is perfectly secret

Proof: Assume that m,c,k are L bits long

- The probability that a bit of c is 1 is $\frac{1}{2}$ no matter what the corresponding bit of m is (because the XOR of any bit with a random bit is random, i.e., has same probability of being 1 as being 0)

- Therefore $\Pr(C=c | M=m) = 2^{-L}$

- $\Pr(C=c) = \sum_{m \in \mathcal{M}} \Pr(C=c | M=m) \Pr(M=m)$

  \[= 2^{-L} (\sum_{m \in \mathcal{M}} \Pr(M=m)) = 2^{-L} = \Pr(C=c | M=m)\]

which is Definition (1) of perfectly secret encryption
Key space size for perfect secrecy

- Perfect secrecy $\Rightarrow |\mathcal{K}| \geq |\mathcal{M}|$ (i.e., size of keyspace $\geq$ size of message space)

**Proof:** Let $f(c)$ be the set of messages $m$ for which some choice of $k$ results in $D_k(c) = m$. If $|\mathcal{K}| < |\mathcal{M}|$ then $|f(c)| < |\mathcal{M}|$ and $\mathcal{M} - f(c)$ is not empty. Let $m^*$ be any message in $\mathcal{M} - f(c)$. We then have:

$$\Pr( M = m^* | C = c ) = 0 \neq \Pr( M = m^* )$$

which contradicts perfect secrecy
Shannon’s Theorem (ShThm)

- An encryption scheme with $|\mathcal{K}|=|\mathcal{M}|=|\mathcal{C}|$ is perfectly secret if and only if:

  1. Key generation is uniform over $\mathcal{K}$ (i.e., the probability that $k \in \mathcal{K}$ is selected is $1/|\mathcal{K}|$)

  2. For every $m \in \mathcal{M}$ and every $c \in \mathcal{C}$, there is a unique $k \in \mathcal{K}$ such that $E_k(m) = c$
Perfect secrecy implies (2) of ShThm

- For a message $m$, let $g(m)$ denote the set of ciphertexts $c$ for which some choice of key $k$ results in $E_k(m) = c$
- $g(m) = C$, else any $c^*$ in $C - g(m)$ satisfies:
  $$\Pr( M=m | C=c^* ) = 0 \neq \Pr( M=m )$$
  contradicting perfect secrecy. Hence $|g(m)| = |\mathcal{K}|$
- $|g(m)| = |\mathcal{K}|$ implies that no two keys $k, k'$ can have $E_k(m) = E_{k'}(m)$, i.e., for an $m, c$ pair a unique key $k$ results in $E_k(m) = c$
Perfect secrecy implies (1) of ShThm

- Let $k$ be the unique key for which $E_k(m) = c$

By perfect secrecy we have:
- $\Pr(C=c \mid M=m) = \Pr(C=c)$

But $\Pr(C=c \mid M=m)$ is $\Pr(K=k)$, therefore:
- $\Pr(K=k) = \Pr(C=c)$

- Repeating the above, for another message $m'$ and the unique key $k'$ for which $E_{k'}(m') = c$, gives:
  - $\Pr(K=k') = \Pr(C=c)$

- Therefore $k$ and $k'$ are equally probable
(1)&(2) in ShThm imply perf. secrecy

- By 2, for every m,c pair there is a unique key k such that $E_k(m)=c$
- $\Pr(C=c \mid M=m) = \Pr(K=k) = 1/|\mathcal{K}|$

where property 1 was used.

- $\Pr(C=c) = \sum_{m \in \mathcal{M}} \Pr(C=c \mid M=m) \Pr(M=m)$
  
  $= \left(1/|\mathcal{K}| \right) \left(\sum_{m \in \mathcal{M}} \Pr(M=m)\right) = 1/|\mathcal{K}|$

- Both $\Pr(C=c)$ and $\Pr(C=c \mid M=m)$ are $1/|\mathcal{K}|$
  which satisfies Defn (3) of perfectly secret encryption