Lecture 07: Graph Representation
Objective

- We shall develop a new graph representation to argue security and correctness of cryptographic schemes.
- As a representative application of this notation, we shall analyze private-key Encryption schemes using graphs.
Assumption about Private-key Encryption Schemes

For simplicity of proof and clarity of the intuition, we shall consider the class of all private-key encryption algorithms with the following restrictions

1. The key-generation algorithm Gen outputs a secret key sampled uniformly at random from the set $\mathcal{K}$
2. The encryption algorithm $\text{Enc}_{sk}(m)$ is deterministic

I want to emphasize that with a bit of effort these restrictions can be removed
Suppose \((Gen, Enc, Dec)\) is a private-key encryption scheme that satisfies the two restrictions we mentioned earlier. We construct the following bipartite graph

- The left partite set is the set of all message \(\mathcal{M}\)
- The right partite set is the set of all cipher-texts \(\mathcal{C}\)
- Given a message \(m \in \mathcal{M}\) and a cipher-text \(c \in \mathcal{C}\), we add an edge \((m, c)\) labeled \(sk\), if we have \(c = Enc_{sk}(m)\)

This is the graph corresponding to the encryption scheme \((Gen, Enc, Dec)\)

**Intuition.** The edge labeled \(sk\) witnesses the fact that the message \(m\) is encrypted to the cipher-text \(c\). Or, we write this as \(m \xrightarrow{sk} c\).

We emphasize that there might be more than one secret key that witnesses the fact that the message \(m\) is encrypted to the cipher-text \(c\). Let \(wt(m, c)\) represent the number of secret keys \(sk\) such that \(sk\) witnesses the fact that \(c\) is an encryption of \(m\).
Describing Private-key Encryption Schemes

- Till now we have represented private-key encryption scheme as a triplet of algorithms \((\text{Gen}, \text{Enc}, \text{Dec})\).
- Henceforth, we can **equivalently** express them as graphs.
Property One: Characterization of Correctness

Theorem

A private-key encryption scheme \((\text{Gen}, \text{Enc}, \text{Dec})\) is incorrect if and only if there are two distinct messages \(m, m' \in \mathcal{M}\), a secret key \(sk \in \mathcal{K}\), and a cipher-text \(c \in \mathcal{C}\) such that \(m \xrightarrow{sk} c\) and \(m' \xrightarrow{sk} c\).

- Note that if there are two message \(m, m'\) such that \(m \xrightarrow{sk} c\) and \(m' \xrightarrow{sk} c\) then Bob cannot distinguish whether Alice produced the cipher text \(c\) for the message \(m\) or \(m'\). Hence, whatever decoding Bob performs, he is bound to be incorrect.

- For the other direction, suppose Bob is unable to decode the \((sk, c)\) correctly. If there is a unique \(m \in \mathcal{M}\) such that \(m \xrightarrow{sk} c\) then Bob can obviously decode correctly. So, there must be two different messages \(m, m' \in \mathcal{K}\) such that \(m \xrightarrow{sk} c\) and \(m' \xrightarrow{sk} c\).
Property Two: Correct Schemes Cannot Compress I

Theorem

A correct private-key encryption scheme \((\text{Gen}, \text{Enc}, \text{Dec})\) has \(|C| \geq |M|\).

- Suppose not. That is, assume that we have a correct private-key encryption scheme with \(|C| < |M|\).
- Fix any secret key \(sk \in \mathcal{K}\).
- Suppose \(M = \{m_1, m_2, \ldots, m_\alpha\}\). Consider the following maps

\[
\begin{align*}
    m_1 & \xrightarrow{sk} c_1 \\
    m_2 & \xrightarrow{sk} c_2 \\
    \vdots \\
    m_\alpha & \xrightarrow{sk} c_\alpha
\end{align*}
\]
Note that these mappings exist because given any sk and $m$ the encryption algorithm maps to a unique cipher-text.

- Since $|C| < |M|$, by pigeon-hole principle there are two distinct messages $m, m' \in M$ and a cipher text $c \in C$ such that $m \xrightarrow{sk} c$ and $m' \xrightarrow{sk} c$

- So the scheme is incorrect. Hence contradiction.
Theorem

A private-key encryption scheme \((\text{Gen}, \text{Enc}, \text{Dec})\) is secure if and only if for any \(c\) and two distinct message \(m, m' \in M\) we have 
\[
\text{wt}(m, c) = \text{wt}(m', c).
\]

For any \(m \in M\) and \(c \in C\), note that we have 
\[
P[C = c|M = m] = \frac{\text{wt}(m, c)}{|\mathcal{K}|}.
\]

Exercise: Prove that the security definition we have studied is equivalent to saying the following

“For any two distinct messages \(m, m' \in M\) and a cipher-text \(c \in C\) we have: 
\[
P[C = c|M = m] = P[C = c|M = m']
\]”

Given this result, we can conclude that a scheme \((\text{Gen}, \text{Enc}, \text{Dec})\) is secure if and only if

“For any two distinct messages \(m, m' \in M\) and a cipher-text \(c \in C\) we have: 
\[
\text{wt}(m, c) = \text{wt}(m', c)
\]”
Food for thought. In a secure scheme, if there are $m \xrightarrow{sk} c$, then for all $m' \in \mathcal{M}$ there exists some $sk'$ such that $m' \xrightarrow{sk'} c$

Food for thought. The size of the set $\mathcal{K}$ need not be divisible by the size of the set $\mathcal{M}$. However, if there is a message $m$ and a cipher-text $c$ such that $wt(m, c) = w$, then the number of secret keys $|\mathcal{K}| \geq w|\mathcal{M}|$. Why?
Theorem

A correct and secure private-key encryption scheme \((\text{Gen}, \text{Enc}, \text{Dec})\) has \(|K| \geq |M|\)

- Suppose not. That is, there is a correct and secure scheme with \(|K| < |M|\).
- Fix a cipher-text \(c \in C\) such that there exists \(m \in M\) and \(sk \in K\) such that \(m \xrightarrow{sk} c\). Intuitively, we are picking a cipher-text that has a positive probability. For example, we are not picking a cipher-text that is never actually produced.
- Let the message space be \(M = \{m_1, m_2, \ldots, m_\alpha\}\)
- Note that, for any \(m_i \in M\) there exists some \(sk_i\) such that \(m_i \xrightarrow{sk_i} c\) (This is a property of secure private-key encryption schemes that was left as an exercise in the previous slide)
Now, consider the mappings

\[ m_1 \xrightarrow{\text{sk}_1} c \]
\[ m_2 \xrightarrow{\text{sk}_2} c \]
\[ \vdots \]
\[ m_\alpha \xrightarrow{\text{sk}_\alpha} c \]

Since \(|\mathcal{K}| < |\mathcal{M}|\), by pigeon-hole principle, there exists two distinct messages \(m_i, m_j\) such that \(\text{sk}_i = \text{sk}_j\) in the above mappings.

This violates correctness. Hence contradiction.
Optimality of One-time Pad

- Note that any correct private-key encryption scheme must have $|C| \geq |M|$ (property two).
- Note that any correct and secure private-key encryption scheme must have $|K| \geq |M|$ (property four).
- One-time pad is a correct and secure scheme that achieves $|K| = |C| = |M|$.
Recall that Property four states that the “correctness and security” of a private-key encryption scheme implies that the size of the set of keys is greater-than-or-equal to the size of the set of messages. For any $M$, construct a correct but insecure private-key encryption scheme such that $|K| = 1!$ This result shall show the necessity of both correctness and security in that property.

Another natural question is: Can we provide such guarantees for private-key encryption schemes that are secure but incorrect? The answer is NO. Think of a private-key encryption scheme that is secure (but incorrect) and works for any message set $M$ and has $|K| = |C| = 1!$