Lecture 04: Properties of Perfect Security

Mathematical Fundamentals: Group

Definition (Group)

For a set G and operator $\circ$, the pair $(G, \circ)$ is a group if it satisfies the following properties:

- Closure: For all $a, b \in G$, we have $a \circ b \in G$
- Associativity: For all $a, b, c \in G$ we have $(a \circ b) \circ c = a \circ (b \circ c)$
- Identity: There exists $e \in G$ such that for all $a \in G$ we have: $e \circ a = a \circ e = a$
- Inverse: For every $a \in G$, there exists $b \in G$ such that we have: $a \circ b = b \circ a = e$

Example of Groups

- Let $G = \{0, 1\}$ and $\circ$ be the XOR operator
- Let $G = \mathbb{Z}$ and $\circ$ be the $+$ operator
- Let $G = \mathbb{Q}^*$ (i.e., the set of all rationals except 0) and $\circ$ be the $\times$ operator
- Let $G = \mathbb{Z}_n = \{0, \dots, n-1\}$ and $\circ$ be the addition $\mod n$ operator
- Let $G = \mathbb{Z}_p^* = \{1, \dots, p-1\}$ (for prime p) and $\circ$ be the multiplication $\mod p$ operator
- Let G be the set of all full-rank $n \times n$ matrices with rational entries and $\circ$ be the matrix multiplication operator
- Given any group $(G, \circ)$ we can define another group $(G^\lambda, \circ^\lambda)$ where G^λ is a λ-long vector with entries in G, and $\circ^\lambda$ is a component-wise application of $\circ$

Note that we have seen examples where G need not be finite and the $\circ$ operator need not be commutative (i.e., $a \circ b = b \circ a$). Groups that additionally satisfy commutativity are called Abelian Groups

One-time Pad

- Let $(G, \circ)$ be a group
- Suppose $\mathcal{K} = \mathcal{M} = \mathcal{C} = G$
- $\mathsf{Gen}(G)$ outputs sk drawn uniformly randomly from G
- $\mathsf{Enc}_{\mathsf{sk}}(m) = m \circ \mathsf{sk}$
- $\mathsf{Dec}_{\mathsf{sk}}(c) = c \circ \mathsf{inv}(\mathsf{sk})$, where $\mathsf{inv}(\mathsf{sk})$ is the inverse of sk with respect to the $\circ$ operator

The proof that one-time pad is perfectly secure is left as an exercise

Thinking Exercises

Proceed by defining meaningful groups $(G, \circ)$ to obtain perfectly secure encryption schemes for the following:

- $\mathcal{M} = \{a, b, \ldots, z\}^\lambda$
- $\mathcal{M} = \{0, 1\}^\lambda$

First Basic Observation

Henceforth, we will restrict our study to encryption scheme that always correctly decrypt, that is:

$$\Pr[\mathsf{Dec}_{\mathsf{sk}}(\mathsf{Enc}_{\mathsf{sk}}(m)) = m] = 1$$

Theorem

For a perfect encryption scheme

$$|\mathcal{C}| \geqslant |\mathcal{M}|$$

Proof:

- Fix any $\mathsf{sk} \in \mathcal{K}$.
- For any distinct $m, m' \in \mathcal{M}$ we cannot have $\mathsf{Enc}_{\mathsf{sk}}(m)$ and $\mathsf{Enc}_{\mathsf{sk}}(m')$ produce the same cipher text c. Otherwise, Bob will not be able to correctly decrypt with probability 1 when it gets (sk, c).

Second Basic Observation

Theorem

For a perfect encryption scheme

$$|\mathcal{K}| \geqslant |\mathcal{M}|$$

Proof:

- Fix a ciphertext c
- For a message $m^{(1)} \in \mathcal{M}$ let $T^{(1)} = \left\{\mathsf{sk}^{(1)}, \dots, \mathsf{sk}^{(i_1)}\right\}$ be the set of all distinct secret keys such that $m^{(1)}$ encrypts to c
- Similarly, for a message $m^{(2)} \in \mathcal{M}$ let $T^{(2)} = \left\{\mathsf{sk}^{(i_1+1)}, \dots, \mathsf{sk}^{(i_2)}\right\}$ be the set of all distinct secret keys such that $m^{(2)}$ encrypts to c
- In general, for a message $m^{(k)} \in \mathcal{M}$ let $T^{(k)} = \left\{\mathsf{sk}^{(i_{k-1}+1)}, \dots, \mathsf{sk}^{(i_k)}\right\}$ be the set of all distinct secret keys such that $m^{(k)}$ encrypts to c

Proof Continued

We make two claims. First claim:

Claim

Let $\mathcal{M}(c)$ be the set of all messages that encrypt to c under some sk*. Then $|\mathcal{M}(c)| = |\mathcal{M}|$.*

Proof:

- If possible let $m \in \mathcal{M}$ such that $m \notin \mathcal{M}(c)$
- Let M be a uniform distribution over $\mathcal{M}$
- Now $\Pr[M = m | C = c] = 0$, but $\Pr[M = m] = 1/|\mathcal{M}| \neq 0$
- So, perfect security is violated

Proof Continued

Second claim:

Claim

For $k \neq k'$, we have $T^{(k)} \cap T^{(k')} = \emptyset$.

Proof:

- Fix c and suppose on the contrary that there exists $\mathrm{sk} \in T^{(k)} \cap T^{(k')}$
- Consider the case when Bob receives the secret-key sk and c as the ciphertext
- In this case, Bob cannot always correctly decrypt the message as both $m^{(k)}$ and $m^{(k')}$ are valid decryptions of the ciphertext c when the secret-key is sk

Proof Continued

Using the two claims we do the following argument:

- Let $\mathcal{M} = \{m^{(1)}, \dots, m^{(S)}\}$
- Then, every set $T^{(1)}, \dots, T^{(S)}$ is non-empty (by first claim). Formally, $i_1 \geqslant 1$, $(i_2 - i_1) \geqslant 1$, $\dots$, $(i_S - i_{S-1}) \geqslant 1$
- Further, $T^{(1)}, \dots, T^{(S)}$ are distinct (by second claim) and their union has size $\leqslant |\mathcal{K}|$
- Consider the following manipulation:

$$\begin{aligned}
|\mathcal{M}| = S = \sum_{k=1}^{S} 1 \\
&\leqslant \sum_{k=1}^{S} (i_k - i_{k-1}) \\
&= i_S \\
&\leqslant |\mathcal{K}|
\end{aligned}$$

- This completes the proof that $|\mathcal{K}| \geqslant |\mathcal{M}|$

Food for Thought

- Observe that One-time Pad achieves $|K| = |M| = |C|$, thus the inequalities in the theorems are tight and can be simultaneously achieved
- Note that the equality in the second theorem is achieved if and only if $(i_k - i_{k-1}) = 1$ and $T^{(1)} \cup \cdots \cup T^{(S)} = \mathcal{K}$. This observation is extremely important will be used extensively in the next theorem's proof

Theorem (Shannon's Theorem)

An encryption scheme is perfectly secure with $|\mathcal{K}| = |\mathcal{M}| = |\mathcal{C}|$ *if and only if*

- Gen *samples* sk *uniformly at random from* $\mathcal{K}$*, and*
- *For every* $m \in \mathcal{M}$ *and* $c \in \mathcal{C}$*, there is a unique* sk *such that* $\mathsf{Enc}_{\mathsf{sk}}(m) = c$

First Direction

Suppose Gen samples sk uniformly at random from $\mathcal{K}$ and for every $m \in \mathcal{M}$ and $c \in \mathcal{C}$, there is a unique sk such that $\mathsf{Enc}_{\mathsf{sk}}(m) = c$. We want to show that this scheme is perfectly secure.

- First guarantee implies: $\Pr[\mathsf{sk} = \mathsf{sk}] = 1/|\mathcal{K}|$, for all $\mathsf{sk} \in \mathcal{K}$
- Fix a c and m. Second guarantee states that there is a unique secret-key under which m is encrypted as c. Let this secret-key be $\mathsf{sk}_{m,c}$. Now,

$$\begin{aligned}
\Pr[C = c | M = m] &= \Pr[C = c \wedge M = m] / \Pr[M = m] \\
&= \Pr[\mathsf{sk} = \mathsf{sk}_{m,c} \wedge M = m] / \Pr[M = m] \\
&= \Pr[\mathsf{sk} = \mathsf{sk}_{m,c}] \cdot \Pr[M = m] / \Pr[M = m] \\
&= \Pr[\mathsf{sk} = \mathsf{sk}_{m,c}]
\end{aligned}$$

- By first guarantee, we can conclude that $\Pr[C = c | M = m] = 1/|\mathcal{K}|$, for all c, m and, hence, the scheme is perfectly secret

Second Direction

Suppose we are given a perfectly secure encryption scheme such that $|\mathcal{K}| = |\mathcal{M}| = |\mathcal{C}|$.

- Fix a ciphertext c
- Because of the tightness of the inequality it is clear that $\left|T^{(k)}\right| = 1$, for all k (we have already argued this earlier). So, for every m, c there is a unique $\mathsf{sk}_{m,c}$ under which m is encrypted as c. This proves the part (2) of the implication
- Further, tightness of the inequality implies that $T^{(1)} \cup \cdots \cup T^{(S)} = \mathcal{K}$, where $S = |\mathcal{M}|$
- Let us consider the following probability for any $m \in \mathcal{M}$:

$$\begin{aligned}
\Pr[C = c | M = m] &= \Pr[C = c \wedge M = m] / \Pr[M = m] \\
&= \Pr[\mathsf{sk} = \mathsf{sk}_{m,c} \wedge M = m] / \Pr[M = m] \\
&= \Pr[\mathsf{sk} = \mathsf{sk}_{m,c}] \cdot \Pr[M = m] / \Pr[M = m] \\
&= \Pr[\mathsf{sk} = \mathsf{sk}_{m,c}]
\end{aligned}$$

Second Direction Continued

- Recall that for perfect secrecy, we must have $\Pr[C = c | M = m]$ identical for all $m \in \mathcal{M}$
- So, for every $m \in \mathcal{M}$, we get $\Pr[\mathsf{sk} = \mathsf{sk}_{m,c}]$ is identical
- Recall that $\mathcal{M} = \{m^{(1)}, \dots, m^{(S)}\}$ and $\left\{\mathsf{sk}_{m^{(1)},c}, \dots, \mathsf{sk}_{m^{(S)},c}\right\} = \mathcal{K}$
- So, we get that $\Pr[\mathsf{sk} = \mathsf{sk}_{m,c}] = 1/\left|\mathcal{K}\right|$. This proves the part (1) of the implication

Food for Thought

- What information is leaked when two messages are encrypted using the same secret-key in one-time pad?
- For example, for two different message (m, m'), their encryptions are (c, c'), where $c = m \circ \mathrm{sk}$ and $c' = m' \circ \mathrm{sk}$
- So, we can compute $c \circ \mathrm{inv}(c')$ to compute $m \circ \mathrm{inv}(m')$
- Is any additional information leaked?
- How to argue that "no additional information" is leaked?