Lecture - 2

Rachit Parikh

February 24, 2022

---

1 Cryptography

What are the uses of cryptography?

- Digital Signatures
- Secure communication
- Integrity

2 Encryption

$\mathbb{K}$ - Key space
$\mathbb{M}$ - Message space
$\mathbb{C}$ - Ciphertext space
$Enc(k, m)$ - Encryption function
$Dec(k, c)$ - Decryption function

2.1 Correctness Property

$Dec(k, Enc(k, m_0)) = m_0$

2.2 Perfect Secrecy

If Bob and Alice are communicating and Eve is eavesdropping, then we have to ensure that she cannot guess the message. Since she can always guess out of message space, we have to make it the worst case. Basically she should not be able to do better than guessing randomly.

First of all we begin with some notation before going to mathematical representation of definition of perfect secrecy.

$Eve(Enc(k, m_0)) = m_0 \rightarrow$ It means that Eve is able to guess the message correctly by looking at the encryption. This is sort of an event or an indicator random variable.

$$X = [Eve(Enc(k, m_0)) = m_b], \text{ where}$$

$X = 1$, if $b = 0$
$X = 0$, if $b \neq 0$

We can now formalize definition of perfect secrecy,

Definition 2.1 (Perfect Secrecy)**.**

$m_0 \xleftarrow{R} \mathbb{M} \quad \implies \quad \Pr[X = 1] \leq \dfrac{1}{|\mathbb{M}|}$

Here, m_0 is selected uniformly from the message space $\mathbb{M}$. By this assumption, every message is equally likely so the best Eve can do is choose a message randomly and hence the above equation should hold if we want our encryption scheme to be perfectly secret.

Corollary 1.

$b \xleftarrow{R} \{0, 1\} \quad \implies \quad \Pr[Eve(Enc(m_b, k)) = m_b] \leq \dfrac{1}{2}$

Here, Eve cannot predict m_0/m_1 by seeing $Enc(m_1, k)$ or $Enc(m_0, k)$

Since the definition $\implies$ corollary, we can also check whether the converse is true. Surprisingly, it is true and can be proven by considering contradiction. To prove Corollary $\implies$ Definition, we can just prove that $\neg$Definition $\implies$ $\neg$Corollary.

Theorem 1. *Corollary 1 $\implies$ Definition 2.1*

Proof. Since we are proving it by contradiction, we just need to show that $\neg$Definition $\implies$ $\neg$Corollary. First, we assume $\neg$Definition.

$$\Pr[Eve(Enc(m_1, k)) = m_1] > \frac{1}{|\mathbb{M}|}$$

Here m_1 is chosen randomly from the message space. Since this is an indicator random variable, we have

$$\mathbb{E}[Eve(Enc(m_1, k)) = m_1] > \frac{1}{|\mathbb{M}|}$$

If we fix m_0, and our only randomness is $k \in \mathbb{K}$, then the probability that $m' = m_1$ can be given as

$$\Pr[Eve(Enc(m_0, k)) = m'] \leq \frac{1}{|\mathbb{M}|}$$

This happens because m_1 is randomly chosen from the message space and the probability of it to be equal to m' is at most $\dfrac{1}{|\mathbb{M}|}$

$$\therefore \mathbb{E}[Eve(Enc(m_0, k)) = m_1] \leq \frac{1}{|\mathbb{M}|}$$

Now, if we take the difference of the random variables,

$$\mathbb{E}[Eve(Enc(m_1, k)) = m_1] - \mathbb{E}[Eve(Enc(m_0, k)) = m_1] > 0$$

This means that the probability of Eve guessing a random m_1 given m_1 is higher than Eve guessing it from some m_0. Hence, for some m_1, we have

$$\Pr[Eve(Enc(m_1, k)) = m_1] > \Pr[Eve(Enc(m_0, k)) = m_1]$$

Hence in the message space $b \xleftarrow{R} \{0, 1\}$,

$$\Pr[Eve(Enc(m_b, k)) = m_b] > \frac{1}{2}$$

Hence, we have proved ¬Corollary 1.

$\square$