Cryptology 25th August, 2015

Lecture 6: Limitations of Perfect Secrecy; Shannon's Theorem

Instructor: Dr. Goutam Paul *Scribe: Abhishek Singh*

1 Limitations of Perfect Secrecy

We show that one of the aforementioned limitations of the one-time pad encryption scheme is *inherent*. We prove that any prefectly-secret encryption scheme must have a key space that is at least as large as the message space.

Theorem 1.1 *Let* (Gen, Enc, Dec) *be a perfectly-secure encryption scheme over a message space* $\mathcal{M}$*, and let* $\mathcal{K}$ *be the key space as determined by* Gen*. Then* $|\mathcal{K}| \geq |\mathcal{M}|$

Proof. We show that if $|\mathcal{K}| \geq |\mathcal{M}|$ then the scheme is not perfectly secret. Let c be a ciphertext that corresponds to a possible encryption of m. Consider the set $\mathcal{M}(c)$ of all possible messages that correspond to c; that is

By assumption, $|\mathcal{M}(c)| \leq |\mathcal{K}| < |\mathcal{M}|$

$$\exists m' \in \mathcal{M} \text{ such that } m' \notin \mathcal{M}(c)$$

This implies,

$$\Pr[M = m'|C = c] = 0 < \Pr[M = m']$$
$$\Pr[M = m'|C = c] \neq \Pr[M = m']$$

This implies the perfect secrecy. □

Lemma 1.2 *For meaningful encryption scheme,* $|\mathcal{C}| \geq |\mathcal{M}|$.

2 Shannon's Theorem

Theorem 2.1 *Let* (Gen, Enc, Dec) *be an encryption scheme over a message space* $\mathcal{M}$ *for which* $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$*. This scheme is perfectly secret if and only if:*

1. *Every key* $k \in \mathcal{K}$ *is chosen with equal probability* $1/|\mathcal{K}|$ *by algorithm* Gen*.*
2. *For every* $m \in \mathcal{M}$ *and every* $c \in \mathcal{C}$*, there exists a single key* $k \in \mathcal{K}$ *such that* $\mathsf{Enc}_k(m)$ *outputs* c*.*

Proof. Let *(Gen, Enc, Dec)* be an encryption scheme over $\mathcal{M}$ where $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$.

(I) Perfect secrecy $\Rightarrow$ Condition 1 and 2 :

We know by Theorem 1.1, that for every $m \in \mathcal{M}$ and $c \in \mathcal{C}$, there exists *atleastone* key $k \in \mathcal{K}$ such that $\mathsf{Enc}_k(m) = c$. For every fixed m, consider now the set,

$$Enc_k(m) = \{c \in \mathcal{C} : \ \exists k \in \mathcal{K} \ such \ that \ Enc_k(m) = c\}$$

By the above,

$$|Enc_k(m)| \geq |\mathcal{C}| \tag{1}$$

(because for every $c \in \mathcal{C}$ there exists a $k \in \mathcal{K}$ such that $\mathsf{Enc}_k(m) = c$).

Since, $\mathsf{Enc}_k(m) \in \mathcal{C}$ we trivially have,

$$|Enc_k(m)| \leq |\mathcal{C}| \tag{2}$$

From 1 and 2, we conclude that,

$$|Enc_k(m)| = |\mathcal{C}| \tag{3}$$

Since $|\mathcal{K}| = |\mathcal{C}|$, it follows that $| \ \mathsf{Enc}_k(m)| = |\mathcal{K}|$. This implies that for every m and c, there do not exists distinct keys $k_1, k_2 \in \mathcal{K}$ with $\mathsf{Enc}_{k_1}(m) = \mathsf{Enc}_{k_2}(m) = c$.
This implies that Condition 2 must be true.

Now, for every $k \in \mathcal{K}$, $\Pr[\mathcal{K} = k] = 1/|\mathcal{K}|$. Let $n = \mathcal{K}$ and $\mathcal{M} = \{m_1, ..., m_n\}$ and fix ciphertext c. By definition of perfect secrecy, we have

$$\begin{aligned} \Pr[M = m_i] &= \Pr[M = m_i \mid C = c] \\ &= \frac{\Pr[M = m_i] \cdot \Pr[C = c_i \mid M = m_i]}{\Pr[C = c_i]} \\ &= \frac{\Pr[M = m_i] \cdot \Pr[K = k_i]}{\Pr[C = c_i]} \end{aligned}$$

From the above, it follows that for every i,

$$\Pr[K = k_i] = \ \Pr[C = c] \tag{4}$$

where k_i maps m_i to c.
Similarly we can show that,

$$\Pr[K = k_j] = \ \Pr[C = c] \tag{5}$$

where k_j maps m_j to c.
From 4 and 5, we get $\Pr[\mathcal{K} = k_i] = \Pr[\mathcal{K} = k_j]$. Similarly,

$$\Pr[K = k_1] = \Pr[K = k_2] = ... = \Pr[K = k_n] = 1/|\mathcal{K}| \tag{6}$$

This implies that condition 1 is true.

(II) Condition 1 and 2 $\Rightarrow$ Perfect secrecy :
Lets consider key space set contains n elements and index each element by $1, 2, 3, ..., n$.

$$\begin{aligned}
\Pr[C = c_i \mid M = m_i] &= \Pr[K = k_i] \; where\ k_i\ maps\ m_i\ to\ c_i\ (from\ Condition\ 2) \\
&= 1/|\mathcal{K}| \; (from\ Condition\ 1) \\
&= \Pr[C = c_j \mid M = m_i],\ j \neq i
\end{aligned}$$

This implies perfect secrecy.
Hence, proved in both directions. □

3 Example of Perfectly Secure Encryption Scheme

3.1 Vernam Cipher(1917)

Vernam Cipher is also called One-Time Pad(OTP), because each message must be encrypted with a different key. The one-time pad encryption scheme is defined as follows:

1. Fix an integer $l > 0$. Then the message space $\mathcal{M}$, key space $\mathcal{K}$, and ciphertext space $\mathcal{C}$ are all equal to $\{0,1\}^l$.
2. The key-generation algorithm Gen works by choosing a string from $\| = \{0,1\}^l$ according to uniform distribution.
3. Encryption Enc works as follows: given a key $k \in \{0,1\}^l$ and a message $m \in \{0,1\}^l$, outputs $c := k \oplus m$.
4. Decryption Dec works as follows: given a key $k \in \{0,1\}^l$ and a ciphertext $c \in \{0,1\}^l$, outputs $m := k \oplus c$.

Let m_i, c_i and k_i be the i^{th} bit of the message, ciphertext and key respectively.
$\forall b \in \{0,1\}$ and $\forall b' \in \{0,1\}$,

$$\begin{aligned}
\Pr[m_i = b \mid c_i = b'] &= \frac{\Pr[m_i = b] \cdot \Pr[c_i = b' | m_i = b]}{\Pr[c_i = b']} \\
&= \frac{\Pr[m_i = b] \cdot \Pr[c_i = b' | m_i = b]}{\sum_j \Pr[m_i = b] \cdot \Pr[c_i = b' | m_i = b]} \\
&= \frac{\Pr[m_i = b] \cdot \Pr[c_i = b' | m_i = b]}{\Pr[m_i = 0] \cdot \Pr[c_i = b' | m_i = 0] + \Pr[m_i = 1] \cdot \Pr[c_i = b' | m_i = 1]} \\
&= \frac{\Pr[m_i = b] \cdot \Pr[k_i = b \oplus b']}{\Pr[m_i = 0] \cdot \Pr[k_i = b'] + \Pr[m_i = 1] \cdot \Pr[k_i = b' \oplus 1]} \\
&= \frac{\Pr[m_i = b] \cdot 1/2}{\Pr[m_i = 0] \cdot 1/2 + \Pr[m_i = 1] \cdot 1/2} \\
&= \Pr[m_i = b]
\end{aligned}$$

This implies perfect secrecy.