Class219: Perfect Secrecy

Virendra Sule

Perfect Secrecy of Encryption

- Encryption methods: Vernam OTP, Block ciphers, Stream ciphers.
- Block and stream ciphers are computationally secure in terms of difficulty of computations of the third property of the TOWF involved in the algorithm.
- Vernam OTP is not secure in the sense of TOWF. But has security due to secrecy and randomness of the symmetric key.
- Security in the sense of Information about the plaintext before and after encryption. Perfect Secrecy.

Information about the plaintext

- Plaintext P is a stream (or a string of alphabets) of a fixed length say N. P belong to the set $\mathcal{P}$ the plaintext space of all strings of length $\leq N$.
- Ciphertext is also a string of alphabets of bounded length $\geq N$. C belongs to the ciphertext space $\mathcal{C}$ of strings of alphabets.
- Symmetric key K is a string of a bounded length of alphabets and belongs to the keyspace $\mathcal{K}$.

DISTRIBUTIONS OVER $\mathcal{P}$, $\mathcal{C}$, $\mathcal{K}$

- $\mathcal{P}$ has a probability distribution $pr(P)$ over its elements P which are plaintexts. For example words such as "Galwan", "Troops", "Mountain" are more probable in a plaintext exchange on Indo-China border than "market", "stalks", "returns" in a typical plaintext of a commercial exchange. Hence there is *a priori* information (probability) about the distribution of plaintexts.
- Once ciphertext C is created, there is a distribution $pr(C)$ of ciphertexts which may depend on key and *a priori* information about the possible plaintext whose ciphertext is C. This probability is denoted $pr(P|C)$ as a conditional probability of an event P given that an event C has occurred.

Note: The analogy with conditional probability is misleading if P, C are not identified as events in the same sample space.

Definition of the notion of Perfect Secrecy

An encryption algorithm (cipher) is said to have *Perfect Secrecy* if

$$pr(P|C) = pr(P)$$

- Thus a perfectly secure cipher reveals no extra information (in terms of change in the a posteriori probability $pr(P|C)$ (than that is already known, the a priori probability $pr(P)$) of a possible plaintext P by knowing the ciphertext C and the distribution $pr(C)$ over $\mathcal{C}$.
- Alternatively a perfectly secure cipher has C independent of P as events.

Cipher $E = (\mathcal{P}, \mathcal{C}, \mathcal{K})$

Consider a cipher $E = (\mathcal{P}, \mathcal{C}, \mathcal{K})$ which denotes an alogrithm

$$C = E(K, P)$$

with spaces of plaintext, ciphertext and keys as denoted.

Theorem

(1949, Shannon) Assume $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$ and $pr(P) > 0$, $pr(C) > 0$ for any P, C. Then E has Perfect Secrecy iff

- *$pr(K)$ is a uniform distribution.*
- *There is a unique K such that $C = E(K, P)$ for any P and given C.*

Only If: E has Perfect Secrecy

- By Baye's theorem the condition for perfect secrecy is equivalent to
$$pr(C|P) = pr(C)$$
for all $P \in \mathcal{P}$ and $C \in \mathcal{C}$.
- The assumption that $pr(C) > 0$ is reasonable since if for some C, $pr(C) = 0$ then C is never used and can be deleted from $\mathcal{C}$.
- Let P be fixed. For each C in $\mathcal{C}$ we have $pr(C|P) = pr(C) > 0$ hence for each $C \in \mathcal{C}$ there must be at least one key K such that $C = E(K, P)$. Hence it follows that $|\mathcal{K}| \geq |\mathcal{C}|$.
- Note, for any encryption we must have $|\mathcal{C}| \geq |\mathcal{P}|$. we are given $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$.

- For each P and C there exists a K such that $C = E(K, P)$. Hence
$$\mathcal{C} = \{C = E(K, P), K \in \mathcal{K}\}$$
But by assumption, $|\mathcal{C}| = |\mathcal{K}|$. Hence there is a unique K such that $C = E(K, P)$ for each given C,P.
- By Baye's theorem
$$pr(P|C) = \frac{pr(C|P).pr(P)}{pr(C)}$$
Since K is unique for each C, P, $pr(C|P) = pr(K)$. Hence from above formula perfect secrecy implies (with the fact $pr(P) > 0$), that
$$pr(K) = pr(C) \text{ for any } K$$
- Also perfect secrecy implies C is independent of P. Hence $pr(K)$ is (constant) uniform and must equal $1/|\mathcal{K}|$.

Let there be unique K such that $C = E(K, P)$ and that $pr(K) = 1/|\mathcal{K}|$. Then

$$\begin{aligned} pr(P|C) &= \frac{pr(P).(1/|\mathcal{K}|)}{\sum_{C=E(K,P)} pr(P).pr(K)} \\ &= \frac{pr(P)/|\mathcal{K}|}{\sum_{P\in\mathcal{P}} pr(P)/|\mathcal{K}|} \\ &= pr(P) \end{aligned}$$

the last step follows because $\sum pr(P) = 1$. Hence E has perfect secrecy.

Vernam cipher (OTP) has Perfect Secrecy

Let $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{0, 1\}^N$. Define $E(K, P)$ by

$$(c_1, c_2, \ldots c_N) = (k_1 \oplus p_1, \ldots, k_N \oplus p_N)$$

where k_i are chosen uniformly randomly from $\{0, 1\}$.

- Then both conditions of the theorem are satisfied and hence OTP has perfect secrecy.
- Since for every session of encryption, the key K has to be chosen uniformly randomly, same K is never used in a different session. Hence OTP also has security against all attacks.
- However the greatest disadvantage of OTP is to have exchanged a unique randomly chosen key for each encryption. Hence OTP poses enormous issue of key management. This is resolved by using TOWFs and resorting to a weaker notion of security in the sense of computational hardness.
- Encryption based on TWOF can never be perfectly secure.