POIS-4

13/01/2023 (Fri)

It is clear that Shannon's perfect secrecy while in theory, is safe, has huge restrictions on it's keyspace (the keyspace has to be bigger than the message space). Therefore we need to relax certain conditions, in order to allow practical communication.

Two (Famous / Necessary) Relaxations to Shannon

We first modify the perfect secrecy definition as follows.
Assume that we now have an adversary model. An adversary chooses two messages, m_0 and m_1 and sends them to the encryption scheme. The encryption scheme as it's subroutine chooses $b \epsilon \{0, 1\}$ and encodes either m_0 or m_1 as $c = enc_k(m_b)$ and sends it back to the adversary. Now the adversary has to decode the job. Now, according to perfect secrecy, there is no extra information leaked about the message in the encryption, and so, the probability of guessing the correct message given the ciphertext should be exactly 50%. Hence we have the following definition

$$\forall\ adversaries\ A$$
$$P(A(c) = b) = \frac{1}{2}$$

Now here are the two relaxations to the perfect secrecy model.

- Instead of all adversaries, we restrict our concern only to practical adversaries
- Instead of having the probabiliy of being able to decode as exactly 1/2, we have it at 1/2 + tolerance

Now we don't really want the adversary to be able to decrypt the message always. Even if it manages to decrypt the message 50-80% of the time, it is still extremely good. Therefore we don't really need deterministic adversary, and probabilitistic adversaries, are as equally good, if not better.

We introduce the concept security parameter, which is a number n, which is a value assumed to be known to any adversary attacking the scheme. The running time of the adversary as well as the adversary's success probabilities are all viewed as functions on n.

We are only concerned with polynomial time adversaries for now, that is, their runtime on decryption, is in polynomial time.

Therefore our definition of perfect secrecy is now as follows.

$$\forall\ PPTM\ adversaries\ A$$
$$P(A(c) = b) = \frac{1}{2} + \text{tolerance}$$

We realize that the tolerance cannot be exactly zero, Therefore we require it to be a negligible function in n.

Negligible Function

A function $f(n)$ is said to be negligible if $\forall$ polynomials p, $\exists n_0$ st $n > n_0$

$$f(n) < \frac{1}{p(n)}$$

Generally speaking , inverse exponential functions (negative exponent) are negligible functions. For example, 2^{-n}.

Hence our updated version of perfect secrecy is.

$$\forall \; PPTM \; adversaries \; A$$
$$P(A(c) = b) = \frac{1}{2} + negl(n)$$

The two conditions are necessary for practical perfect secrecy, and are almost sufficient, we however need one more tool- One way functions. If we manage to prove that One-way functions exist, this definition is as good as pure perfect secrecy. We also have Trapdoor one-way functions, which are one-way functions with an additional requirement - that inverse calculation becomes easy, when some extra info (called the trapdoor information) is revealed.
One-way functions have opened the way for *MACs*, whereas *Public key cryptography* would be impossible without trapdoor one-way functions.

Different types of attack (refer to AKD notes later ig)

- Ciphertext only attack
- Known Plaintext attack
- Chosen Plaintext attack
- Chosen Ciphertext attack

Different Types of security

Heuristic Security (No proof for perfect secrecy, computational checks confirm it works)

- DES
- AES
- RC4
- RC6
- MD5

Provable Security

Requires us to prove that one-way functions exist

Proven Security (no need to prove one way functions exist)

- One-Time Pad