CCA-secure encryption scheme

Sarthak Mahajan, 2018111005

March 7, 2022

1 CCA Attacks:

CCA(Chosen Cipher text Attack) is an attack in which the adversary has access to both the encryption and decryption servers, and can get decryption of chosen ciphertexts as well as encryption of chosen plaintexts.

2 Definition of CCA Security:

Assume that the Adversary has access to both the encryption and decryption servers, and it sends two messages m_0 and m_1 (of same length) to the encryption algorithm and the encryption algorithm sends it an encryption of message m_b back(chosen randomly), where b = 0 or 1. Let b_{guess} be adversary's guess of which message is sent. Then the Cryptosystem is CCA-secure if for all PPT(probabilistic polynomial time) adversaries A:

$$P\left[b_{\text{guess}} = b\right] <= 1/2 + \text{ negl}(\ n\ )$$

3 CCA Security:

3.1 Idea:

For CCA security, the sender first encrypts the message m to c(using a CPA secure scheme), then makes a tag t of this cipher c using MAC_k, and sends (c, t) to the receiver.At the receiver's side, the receiver first verifies if the tag t is valid by comparing the $MAC_k(c)$) with t, if they are equal the message is accepted, otherwise rejected. If the message is accepted, receiver applies the CPA-secure decryption on the cipher received to obtain the message m.The MAC and CPA encryption have separate keys.The reason this works is because now the Adversary can't access decryption server as he would fail the message authentication unless adversary has the ciphertext from the encryption server from an earlier instance, but since the message is CPA secure encrypted even that won't work.

3.2 CCA Security using MAC and CPA security:

Let $\Pi_E = (\text{Gen}_E, \text{Enc}, \text{Dec})$ be a private-key encryption scheme and let $\Pi_M = (\text{Gen}_M, \text{Mac}, \text{Vrfy})$ be a message.authentication code. Define a CPA-secure encryption scheme (Gen', Enc', Dec') as follows:

- Gen': on input 1^n, run $\text{Gen}_E(1^n)$ and $\text{Gen}_M(1^n)$ to obtain keys k_1, k_2, respectively.
- Enc': on input a key (k_1, k_2) and a plaintext message m, compute $c \leftarrow \text{Enc}_{k_1}(m)$ and $t \leftarrow \text{Mac}_{k_2}(c)$ and output the ciphertext $\langle c, t \rangle$
- Dec': on input a key (k_1, k_2) and a ciphertext $\langle c, t \rangle$, first check whether $\text{Vrfy}_{k_2}(c, t) \stackrel{?}{=} 1$. If yes, then output $\text{Dec}_{k_1}(c)$; if no, then output 1 .