1 CCA-Security

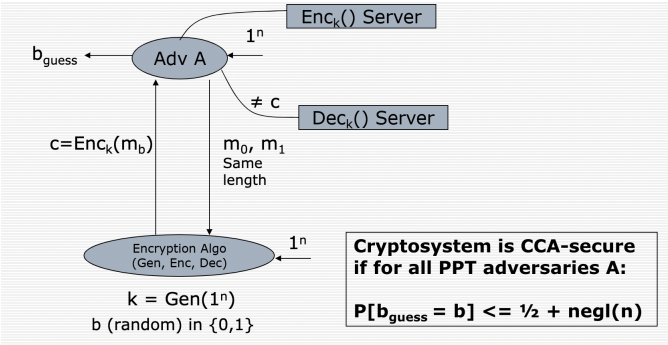

Figure 1: CCA-Security scheme

1.1 Chosen Cipher-text Attack

Here we assume that the adversary has access to both encryption server as well as decryption oracle. A chosen-ciphertext attack (CCA) is an attack model where adversary can gather information by obtaining the decryptions of chosen ciphertexts. From these pieces of information, the adversary can attempt to recover the hidden secret key used for decryption.

1.2 Does Encryption guarantee Integrity?

Encryption does not guarantee integrity. These two are different things. An attacker can modify the cipher in transit and it will hamper the integrity of the message. So we need a way to authenticate messages that are being sent.

1.3 Designing CCA-Security Scheme

$$c = (r, F_{k1}(r)+m), MAC_{k2}(r, Fk1(r)+m)$$

Figure 2: CCA- encryption cipher scheme

The main crux of this encryption is to first encrypt, then authenticate. While receiving, if the authentication is not passed, we simply do not need to perform redunt decryption of some modified message. If it passes authentication, then we decrypt it.
Mathematically,

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

- Gen': on input 1^n, we 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, we compute $c \leftarrow \text{Enc}\ k1(m)$ and $t \leftarrow \text{Mac}\, k2(c)$ and output the ciphertext $\langle c, t)$

- Dec: on input a key (k_1, k_2) and a ciphertext $\langle c, t)$, first we check whether $V_{rfy} k_2(c, t) \stackrel{?}{=} 1$. If yes, then output $\text{Dec}\, k1(c)$; if no, then output 1 .