CCA

February 22, 2023

Assuming our MAC and CPA are secure.

To prove:

For all PPTM Adversary A given two messages m_0 and m_1 and an encryption $E(m_r)$ of a random message m_r between m_0 and m_1, A cannot determine which message (m_0 or m_1) was encrypted.

Proof: Let $C = E(m_r)$ be the encryption of the random message m_r, and let C' be any other ciphertext except C.

Let B be a PPTM that can distinguish between encryptions of m_0 and m_1 with non-negligible advantage.

Then we can construct an attacker A' that can break semantic security of the encryption scheme, as follows:

A' is given C and C', and uses C as the encryption of m_r and C' as any other ciphertext. A' runs B on (m_0, m_1, C) and obtains the output bit b. A' outputs b as its guess for whether C was encrypted under m_0 or m_1. Since B has non-negligible advantage, the probability that A' outputs the correct guess is non-negligible as well. Therefore, the encryption scheme is not semantically secure, which contradicts our assumption.

Thus, we have proven that for all PPTM Adversary A, given two messages and an encryption of one random message between the two, A cannot determine the original message with non-negligible advantage.

Alternate proof: For all PPTM Adversary A given two messages m_0, m_1 and an encryption c of one random message m_b between the two, the adversary should not be able to figure out the original message. A can also query any other ciphertext other than c to a decryption Oracle O to get its decryption.

$$Pr(A(c) = b; \text{s.t } c \notin Q) \leq negl(n)$$

Proof

Assuming our MAC is secure and enc scheme is CPA secure, our construction will only return decryption if decrypted message and tag are valid message-tag pair. Since we proved the security of MAC,

$$Pr(\text{Vrfy}(< m, t >) = 1 | m \notin Q) \leq negl(n)$$

Hence,

$$Pr(\text{ValidQuery}) \leq negl(n)$$

This hides our decryption oracle since the adversary cannot produce a valid query. And since our encryption scheme is also CPA secure, any CPA attack also does not work. Therefore,

$$Pr(A(c) = b; \text{s.t } c \notin Q) \leq negl(n)$$

Thus, the statement is proved.