CPA

February 22, 2023

Assuming a CPA-secure encryption scheme, we want to prove that CPA is provably secure.

We will assume that the attacker A makes polynomial queries and show that this is not possible.

Suppose there is an attacker A that can break the CPA security of the encryption scheme. Then, there must exist two messages m_0 and m_1 such that A can distinguish between the encryptions $Enc(m_0)$ and $Enc(m_1)$ with non-negligible advantage. Let b be the bit that A outputs.

We will now construct an attacker B that can break the security of the encryption scheme using A as a subroutine. B works as follows:

1. B generates two messages m_0 and m_1.
2. B selects a random bit $r \in 0, 1$ and computes $c = Enc(m_r)$.
3. B runs A on c and outputs A's output b'. If $b' = r$, then B outputs m_0. Otherwise, B outputs m_1.

Now, we need to analyze the advantage of B. Let Adv_A be the advantage of A in distinguishing between the encryptions $Enc(m_0)$ and $Enc(m_1)$, and let Adv_B be the advantage of B in guessing r correctly.

We have:

$$\begin{aligned} Adv_B &= Pr[B \text{ outputs the correct } m_r] \\ &= Pr[A \text{ outputs the correct } b' | c = Enc(m_r)] \\ &= Pr[A \text{ outputs } r | c = Enc(m_r)] \\ &= \frac{1}{2} + \frac{Adv_A}{2} \end{aligned}$$

This follows because A has a non-negligible advantage in distinguishing between $Enc(m_0)$ and $Enc(m_1)$, so its advantage in guessing r correctly is at most $\frac{1}{2} + \frac{Adv_A}{2}$.

Since A is polynomial, B is also polynomial. Therefore, if A can break the CPA security of the encryption scheme with non-negligible advantage, then B can guess r with non-negligible advantage. But this contradicts the assumption that the encryption scheme is CPA-secure.

Therefore, CPA is provably secure.