EAV

February 22, 2023

Consider a cryptosystem that is secure under the assumption of semantic security, which means that given an encryption c of a random message m, an adversary cannot distinguish whether c was obtained by encrypting m or encrypting a different random message.

Let m_0 and m_1 be two random messages, and let c be an encryption of one of them. Assume that there exists a PPTM adversary A that can correctly guess which message was encrypted with probability $p > 1/2$.

Proof By Contradiction:

Let us construct a new adversary A' that simulates A and outputs the opposite guess with probability $1-p$. Specifically, if A guesses that m_0 was encrypted, A' outputs m_1 as the original message, and if A guesses that m_1 was encrypted, A' outputs m_0 as the original message. Note that A' is also a PPTM adversary.

Since the cryptosystem is semantically secure, the probability that A' guesses correctly is also $p > 1/2$, and the probability that A' guesses incorrectly is $1 - p < 1/2$. Therefore, we have constructed an adversary A' that violates the assumption of semantic security, and this is a contradiction.

Thus, we can conclude that any PPTM adversary A that is given two messages m_0 and m_1 and an encryption c, one of them cannot guess the original message with probability significantly greater than $1/2 + negl(n)$, where $negl(n)$ is a negligible function of the security parameter n. Hence, proved.

Alternate proof:

For any probabilistic polynomial-time (PPTM) adversary A, if we are given two messages m_0 and m_1, and an encryption c of one of these messages, the adversary should not be able to determine the original message with a probability significantly greater than $1/2 + negl(n)$, where $negl(n)$ is a negligible function of the security parameter n.

$$\Pr[A(c) == b] = \frac{1}{2} + \mathrm{negl}(n)$$

If we take D as a PPTM which outputs 0 or 1,

$$Pr_{w \leftarrow 0,1^{1(n)}}[D(w) = 1] = 1/2$$

let G be a pseudo random number generator

$$\Pr_{s \leftarrow \{0,1\}^n}[D(G(s)) = 1] \leq 1/2 + \mathrm{negl}$$

This implies,

$$\Pr_{s\leftarrow\{0,1\}^n}[D(m\oplus G(s))=1]\leq 1/2+\text{negl}(n)$$

Therefore,

$$Pr_{w\leftarrow 0,1^{1(n)}}[D(c)=1]\leq 1/2+\text{negl}(n)$$

Hence, this completes the proof that any PPTM adversary A that is given two messages m_0 and m_1 and an encryption c, one of them cannot guess the original message with probability significantly greater than $1/2+negl(n)$, where $negl(n)$ is a negligible function of the security parameter n.