CCA SECURE ENCRYPTION SCHEME CONCEPTS

Overview:

In a chosen-ciphertext attack, an adversary causes a receiver to decrypt ciphertexts that it generates.

A scheme that is CCA- secure is defined below:

DEFINITION 5.1 *A private-key encryption scheme* Π *has* indistinguishable encryptions under a chosen-ciphertext attack, *or is* CCA-secure, *if for all*

probabilistic polynomial-time adversaries $\mathcal{A}$ *there is a negligible function* negl *such that:*

$$\Pr[\mathsf{PrivK}^{\mathsf{cca}}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathsf{negl}(n),$$

where the probability is taken over all randomness used in the experiment.

Code construction:

Code construction follows the scheme given below.

CONSTRUCTION 5.6

Let $\Pi_E = (\mathsf{Enc}, \mathsf{Dec})$ be a private-key encryption scheme and let $\Pi_M = (\mathsf{Mac}, \mathsf{Vrfy})$ be a message authentication code, where in each case key generation is done by simply choosing a uniform n-bit key. Define a private-key encryption scheme $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ as follows:

- Gen': on input 1^n, choose independent, uniform $k_E, k_M \in \{0,1\}^n$ and output the key (k_E, k_M).
- Enc': on input a key (k_E, k_M) and a plaintext message m, compute $c \leftarrow \mathsf{Enc}_{k_E}(m)$ and $t \leftarrow \mathsf{Mac}_{k_M}(c)$. Output the ciphertext $\langle c, t\rangle$.
- Dec': on input a key (k_E, k_M) and a ciphertext $\langle c, t\rangle$, first check if $\mathsf{Vrfy}_{k_M}(c, t) \stackrel{?}{=} 1$. If yes, output $\mathsf{Dec}_{k_E}(c)$; if no, output $\perp$.

This is commonly known as Encrypt then Authenticate scheme

Proof:

Encrypt-then-authenticate. In this approach, the message is first encrypted and then a MAC is computed over the result. That is, the ciphertext is now the pair $\langle c, t\rangle$ where

$$c \leftarrow \mathsf{Enc}_{k_E}(m) \quad \text{and} \quad t \leftarrow \mathsf{Mac}_{k_M}(c).$$

Decryption of $\langle c, t\rangle$ outputs an error if $\mathsf{Vrfy}_{k_M}(c, t) \neq 1$, and otherwise outputs $\mathsf{Dec}_{k_E}(c)$. See Construction 5.6 for a formal description.

This approach *is* sound. As intuition for why, say a ciphertext $\langle c, t\rangle$ is *valid* if t is a valid tag on c. Strong security of the MAC ensures that an adversary will be unable to generate *any* valid ciphertext that it did not receive from its encryption oracle. This immediately implies that Construction 5.6 is unforgeable. Moreover, it effectively renders the decryption oracle useless: for every ciphertext $\langle c, t\rangle$ the adversary submits to its decryption oracle, the adversary either already knows the decryption (if it received $\langle c, t\rangle$ from its encryption oracle) or will receive an error. (Observe also that the tag is verified before decryption takes place; thus, errors during decryption cannot leak anything about the plaintext, in contrast to the padding-oracle attack we saw against the authenticate-then-encrypt approach.) Therefore, CCA-security of the combined scheme reduces to CPA-security of Π_E.