CCA

In order to achieve CCA-security, we will construct an encryption scheme with the property that the adversary will not be able to obtain any valid ciphertext that was not generated by the legitimate parties. This will have the effect that the decryption oracle will be rendered useless. Given this intuition, it is clear why message authentication codes help. Namely, our construction works by first encrypting the plaintext message, and then applying a MAC to the resulting ciphertext. This means that only messages generated by the communicating parties will be valid (except with negligible probability).

Let $\Pi_E = (\mathsf{Gen}_E, \mathsf{Enc}, \mathsf{Dec})$ be a CPA-secure encryption scheme and $\Pi_M = (\mathsf{Gen}_M, \mathsf{Mac}, \mathsf{Vrfy})$ a secure message authentication code. The construction is as follows:

CONSTRUCTION 4.17 CCA-secure encryption.

Define a CCA-secure encryption scheme as follows:

- $\mathsf{Gen}'(1^n)$: upon input 1^n, choose $k_1, k_2 \leftarrow \{0,1\}^n$
- $\mathsf{Enc}'_k(m)$: upon input key (k_1, k_2) and plaintext message m, compute $c = \mathsf{Enc}_{k_1}(m)$ and $t = \mathsf{Mac}_{k_2}(c)$ and output the pair (c, t)
- $\mathsf{Dec}'_k(c, t)$: upon input key (k_1, k_2) and ciphertext (c, t), first verify that $\mathsf{Vrfy}_{k_2}(c, t) = 1$. If yes, then output $\mathsf{Dec}_{k_1}(c)$; if no, then output $\perp$.

Assume that Π E = (GenE , Enc, Dec) is a CPA-secure encryption scheme and that ΠM = (GenM , Mac, Vrfy) is a secure message authentication code with unique tags. Then, Construction 4.17 is a CCA-secure encryption scheme.

The idea behind the proof of this theorem is as follows. Since (Gen M , Mac, Vrfy) is a secure message authentication code, we can assume that all queries to the decryption oracle are invalid, unless the queried ciphertext was previously obtained by the adversary from its encryption oracle. Therefore, the security of the scheme Π0 = (Gen0, Enc 0, Dec0) in Construction 4.17 is reduced to the CPA-security of (GenE , Enc, Dec) (because the decryption oracle is effectively useless).

Can we use the variable-length MAC construction as defined in Section 5?
Answer: It is generally not recommended to use variable-length MAC constructions, instead of CBC-MAC to implement CCA (chosen-ciphertext attack) security for

encryption schemes, as these constructions are not designed for this purpose and may not provide the same level of security guarantees.

CBC-MAC (Cipher Block Chaining Message Authentication Code) is a deterministic message authentication code that uses a block cipher to process fixed-length blocks of data. It is specifically designed to provide message authentication, and its security proof assumes that the attacker does not have access to the encryption oracle. However, it is vulnerable to chosen-ciphertext attacks, which can allow an attacker to construct new valid MACs for messages that have not been previously authenticated.

Although, variable length MAC can also provide message authentication, they are not designed to provide CCA security. In particular, they do not have the same security properties as CTR mode or GCM mode and may be vulnerable to attacks that exploit their construction. Therefore, it is generally not recommended to use HMAC or CMAC instead of CBC-MAC for achieving CCA security in an encryption scheme.