2021201041
Nvss Maneesh Gupta

How CCA security is achieved from CBC-MAC

"Encrypt and then authenticate"

$$c = \left(r, F_{k_1}(r) + m\right), MAC_{k_2}(r, F_{k_1}(r) + m)$$

Where

- r is the random noise used for CPA security
- K1 is the key for PRF
- F is the PRF
- m is plain text message
- k_2 is the key for CBC-MAC

Here encryption is done CPA security (confidentiality) and the authentication is done for CCA security (integrity)

CONSTRUCTION 4.19

Let $\Pi_E = (\mathsf{Gen}_E, \mathsf{Enc}, \mathsf{Dec})$ be a private-key encryption scheme and let $\Pi_M = (\mathsf{Gen}_M, \mathsf{Mac}, \mathsf{Vrfy})$ be a message authentication code. Define an encryption scheme $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ as follows:

- Gen': on input 1^n, run $\mathsf{Gen}_E(1^n)$ and $\mathsf{Gen}_M(1^n)$ to obtain keys k_1, k_2, respectively.
- Enc': on input a key (k_1, k_2) and a plaintext message m, compute $c \leftarrow \mathsf{Enc}_{k_1}(m)$ and $t \leftarrow \mathsf{Mac}_{k_2}(c)$ and output the ciphertext $\langle c, t \rangle$
- Dec': on input a key (k_1, k_2) and a ciphertext $\langle c, t \rangle$, first check whether $\mathsf{Vrfy}_{k_2}(c, t) \stackrel{?}{=} 1$. If yes, then output $\mathsf{Dec}_{k_1}(c)$; if no, then output $\perp$.

A CCA-secure private-key encryption scheme.

References

[1] J. K. a. Y. Lindell, Introduction to Modern Cryptography.

[2] B. Micali, "Hardcord bits," [Online]. Available: https://crypto.stanford.edu/pbc/notes/crypto/hardcore.html.

[3] Lecture Slides