How CCA security is achieved from CBC-MAC

“Encrypt and then authenticate”

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
* k2 is the key for CBC-MAC

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



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