

M.Duclos, Y.Alboloushi, M.Alnuaimi, F.Devillez, H.Raeisi

## A Concrete Security Treatment of Symetric Encryption [1]

### Abstract

This paper proposes to define several notions of security. This notions will be applicated only on symmetric encryption scheme specily in a concrete security framework.

The first notion is Left-or-Right Indistinguishability which considers two string with the same lenght  $x_0$  and  $x_1$  and a left-or-right oracle. To summarize, we take a bit  $b$  and encrypt  $x_0$  if  $b=1$  or  $x_1$  if  $b=0$ . The challenge for the adversary is to guess the value of  $b$ . The second notion is Real-or-Random Indistinguisability. The idea is that an adversary cannot distinguish an encrypted text with an encryption of an equal-lenght string of garbage. Then, we have the Find-then-Guess Security which is an adaption of the polynomial security. The last notion is semantic security, It is presented saying that whatever can be efficiently computed about a plaintext given the cyphertext can also be computed in absence of the ciphertext.

For each notions, we have a study of the concrete complexity of reductions between the different notions. For each notions, upper and lower bounds of complexity to establish relations between them and comparing them in order to define the strongest or the weakest. 7 different proofs of reduction, permit to classify the different notion, and make a scheme to summarize this.

Like it is claimed on the goal of the paper, the different new notions of security are created in order to have concrete analyse of symmetric schemes. The second party of the paper is an analyse of three different scheme, wich have never received formal analyse at the time of the paper. The three different modes of encrption with a bloc cypher (*e.g.* DES) are CBC (Cipher Block chazing mode), CTR (Counter mode) and XOR (variant of CTR). To prove bounds of security in this different schemes, we need also some explanations on pseudorandom function (PRF) and Pseudorandom Permutation function(PPF) families.

### References

- [1] Mihir Bellare, Anand Desai, Eron Jokipii, and Phillip Rogaway. A concrete security treatment of symmetric encryption. In *FOCS '97: Proceedings of the 38th Annual Symposium on Foundations of Computer Science*, page 394, Washington, DC, USA, 1997. IEEE Computer Society.