Contents

Lesson 11

4.1 Authenticated encryption (Age of Ultron)

Last time we proved CPA-security of Π. Today we will explore the *auth* property. Consider Π as

$$Enc : \{0,1\}^\lambda * \mathcal{M} \to \mathcal{C}$$
$$Tag : \{0,1\}^\lambda * \mathcal{C} \to \Phi$$

Lemma 1. *If* $Tag(.,.)$ *is* ***EUF-CMA*** *, then* Π *has auth-property.* ◇

What is **EUF-CMA** ?
It's a property similar to **uf-cma** , but now I want that the challenge message (m^*, ϕ^*) is made by a fresh m^* and a valid **fresh** ϕ^*.
The difference is that in ufcma we didn't care about the freshness of ϕ^*.

Proof. Suppose Π has not the *auth* property.
So we have an $\mathcal{A}'$ which can win the **auth** challenge of Π.
On the other hand, we have a Π_2 schema which uses an **euf-cma** $Tag(.,.)$ function.
So, by reduction, we show that ...

□