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.* $\diamond$

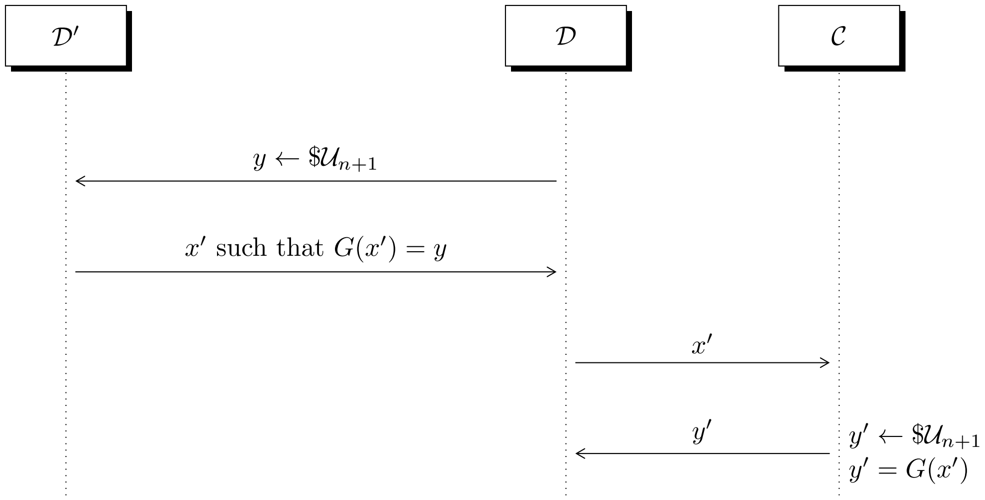
What is **EUF-CMA** ?
It's a property similar to **uf-cma** , but now I want that the challenge message (m^*, ϕ^*) is made by a fresh m^* and a valid **fresh** ϕ^*.
The difference is that in ufcma we didn't care about the freshness of ϕ^*.

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 ...

$\square$

Exercise 3 - point a

We define a *Game*, supposing y is correctly chosen among the G codomain (and this happens with probability equal to $\frac{1}{2}$):



Now D can check if $y = y'$, and can win against C. Since D and D' work in polyλ, we can state that D can distinguish in polyλ this PRG from $\mathcal{U}_{n+1} \Rightarrow G$ is not a PRG, but this is a contraddiction with initial statement.

Exercise 4 - point a

From the security of ONE-TIME pad , if you have some arbitrary distribution D over a group G, and the uniform distribution U over the same group G.
If D and U are independent, we have that $y \leftarrow \$U$ and $x \leftarrow \$D$, and computing $z = x \oplus y$ we have that z is distributed uniformly over G.
Thus, in the end I build

$$G^*(x, x') = G_1(x) \oplus G_2(x')$$

for $x \neq x'$.

Now , we want to show that, given a PRG G_1 and a non-PRG G_2, $G(x) = G_1(x) \oplus G_2(x)$ is a PRG.
We want to show , by contraddiction, that G is always a PRG. Now suppose that we have the following game, where the PRG function is G_1:

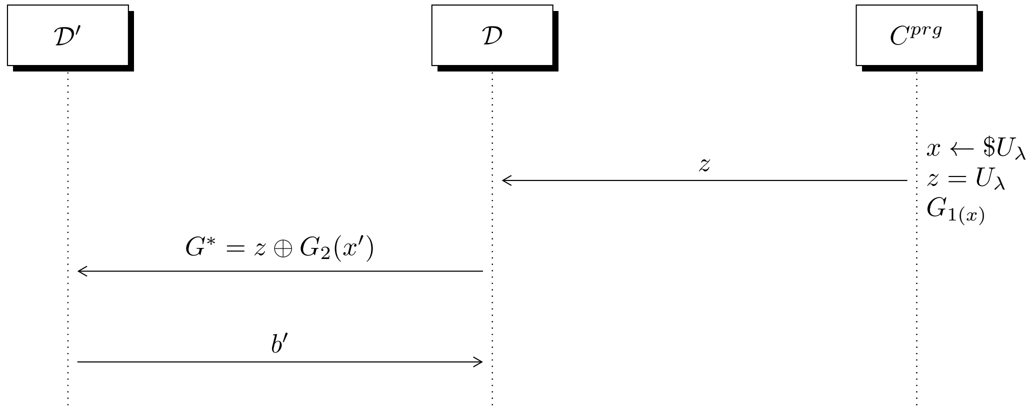
, with $x' \leftarrow \$\{0,1\}^\lambda$ and G_2 such that its output is always equal to identity string. Then $G^* = z \oplus G_{2(x')} = z$ always. Now D wins over C^{prg} , but this is a contraddiction since PRG cannot be distinguished from random extraction.
Furthermore, since the same reduction can be built for the case when G_2 is the PRG one, we can state that G is always a PRG.

Exercise 4 - point b[1]

We can demostrate that optimal seed length is 2λ because in the following case:

$$G^*\{0,1\}^\lambda$$

[1] da rivedere bene



we obtain

$$G^*(x) = G_1(x) \oplus G_2(x)$$

.
And in this case G^* is not perfect