Lezione 13

venerdì 10 novembre 2023 11:11

PSEUDO RANDOM PERMUTATION

Recap: PRF implies EFFICIENTLY everything in symmetric crypto.
Sometimes need PRP (i.e. modes of operations).

we can't prove much

From theory: OWF ⇒ PRF, (⇒ PRP) we'll see Today.

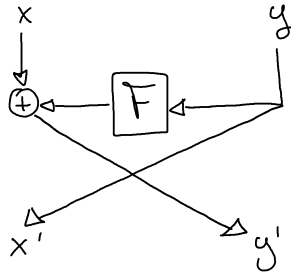
From practise: AES is a PRP. Make some ad-hoc PRF (only heuristic) and then use construction PRF ⇒ PRP

there is a famous one so it's pseudorandom and invertible.

LUBY-RACKOFF construction

$F: \{0,1\}^n \to \{0,1\}^n$ (not invertible)

construction: $\Psi_F(x,y) = (y, x \oplus F(y)) = (x', y')$



who invented it

(FIESTEL)

now it's $\{0,1\}^{2n} \to \{0,1\}^{2n}$

and we claim it's invertible even if F it's not:

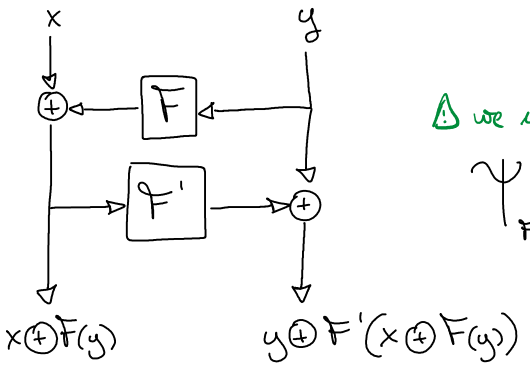
$$\Psi_F^{-1}(x', y') = (F(x') \oplus y', x') = (x, y)$$

• Question: is it pseudorandom? Assuming F it is. NO

2° part of the output exactly the 1° part of the input

If this happens we can say for sure that it's FIESTEL and not R

We can use this construction multiple times
Try 2 ROUNDS



⚠ we use different functions

$$\Psi_{F,F'}(x,y) = \Psi_{F'}(\Psi_F(x,y))$$ still invertible

• Question: Is it a PRP? NO

We can break it with 2 queries: (x,y) and (x',y) $x \neq x'$
so we get $\Psi_{F,F'}(x,y)$ and $\Psi_{F,F'}(x',y)$

$(x \oplus F(y)) \oplus (x' \oplus F(y))$

If we XOR them: $\Psi_{F,F'}(x,y) \oplus \Psi_{F,F'}(x',y) = (x \oplus x', \_\_\_\_\_)$

So we can check.

LUCKY - RACKOFF: $\boxed{\text{3-ROUND WORKS}}$

Thm

Let $\mathcal{F}$ be a PRF.

Then $\Psi_{\mathcal{F}}[3] = \Psi_{F_{k_3}}(\Psi_{F_{k_2}}(\Psi_{F_{k_1}}(x,y)))$ it's a PRP

for $k_1, k_2, k_3 \leftarrow \$ \{0,1\}^{\lambda}$

Practice: $\mathcal{F}$ replaced by heuristic construct (S-BOXES) # of rounds: like 18 times

$k_1, \dots, k_{18}$ all derived from single k

Two steps:

1. If the queries have all y unique then 2-ROUND FESTEL is secure.
2. the first round makes all queries "y"-NIQUE (all y unique)

LEMMA: For every UNBOUNDED distinguisher asking $q(\lambda) = poly(\lambda)$ queries, the following are close: STATISTICALLY

→ S: $F, F' \leftarrow \$ \mathcal{R}(\lambda, n, n)$

and answer (x,y) with $\Psi_{F'}(\Psi_F(x,y))$

→ R: $R \leftarrow \$ \mathcal{R}(\lambda, 2n, 2n)$

and answer (x,y) with $R(x,y)$

so long as $(x_1, y_1), \dots, (x_q, y_q)$ are s.t. $\overbrace{y_i \neq y_j \quad \forall i \neq j}^{\text{y-NIQUE}}$.

proof: Hybrid argument : $H_i(\lambda)$ that answers the first i queries using S and all other queries using R. We already know: $H_0 \equiv R$ and $H_q \equiv S$

(we need to prove $H_i \approx_s H_{i-1}$).

The first i outputs of H_i: 2 ROUND FIESTEL

$$\left(x_j \oplus F(y_j),\ y_j \oplus F'(x_j \oplus F(y_j))\right)_{j=1}^{i-1},$$

$$x_i \oplus F(y_i),\ y_i \oplus F'(x_i \oplus F(y_i)), \dots, \dots, \dots$$

at a certain point he will answer R

By the y-NIQUENESS, $F(y_i)$ is random and independent of the rest.

By the y-UNIQUENESS, $F(y_i)$ is random and independent of the rest: so we can write

$$\left(x_j \oplus F(y_j),\ y_j \oplus F'(x_j \oplus F(y_j))\right)_{j=1}^{i-1},$$

$$\boxed{\left(x_i \oplus r,\ y_i \oplus F'(x_i \oplus r)\right)},\ ---,\ ---,\ ---$$

What's now the probability that $x_i \oplus r = x_j \oplus F(y_j)$?

For some $j < i$ the probability $\leq (i-1)\cdot 2^{-m}$. Assuming it doesn't happen:

this becomes

$$\left((x_i \oplus r), (y_i \oplus r')\right) \text{ which is } \equiv R(x_i, y_i) \text{, uniform}$$

By the lemma of game playing the distance between H_i and $H_{i-1} \leq \underbrace{q(\lambda)}\cdot 2^{-m} = negl(\lambda)$.

To be precise it should be $(i-1)$

$$\Delta(S; R) \leq \sum (i-1)\cdot 2^{-m} \leq q^2 \cdot 2^{-m} = negl(\lambda)$$

$\boxtimes$ lemma

proof (Thm)

We consider a bunch of experiments.

2 exp.
- $T: (x,y) \longmapsto \Psi_{F_{k_3}}(\Psi_{F_{k_2}}(\Psi_{F_{k_1}}(x,y)))$ real world.
- $S: (x,y) \longmapsto \Psi_{F,F'}(\Psi_{F''}(x,y))$ Truly 3 random function: $F, F', F'' \leftarrow \$ \mathcal{R}(\lambda, m, m)$
- $R: (x,y) \longmapsto R(x,y)$ $\quad R \leftarrow \$ \mathcal{R}(\lambda, 2m, 2m)$ RANDOM FUNCTION

ideal world RANDOM PERMUTATION
- $P. (x,y) \longmapsto P(x,y)$ $\quad P \leftarrow \$ \mathcal{P}(\lambda, 2m, 2m)$ RANDOM PERMUTATION

We want to demonstrate that they are all indistinguishable.