

BLOCK CIPHERS

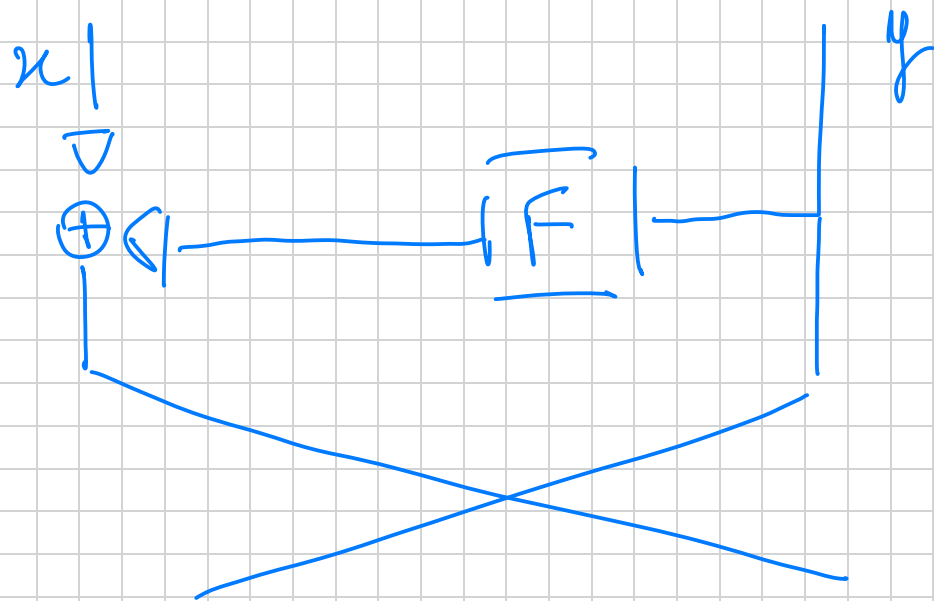
But the name is MISLEADING. Actually,

They are PSEUDORANDOM PERMUTATIONS.

Examples; DES, AES, ... They are used often as an instantiation of a PRF, but they are more as they are INVERTIBLE.

We already have a PRF, how do we make it invertible. Most famous design: FEISTEL NETWORKS.

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



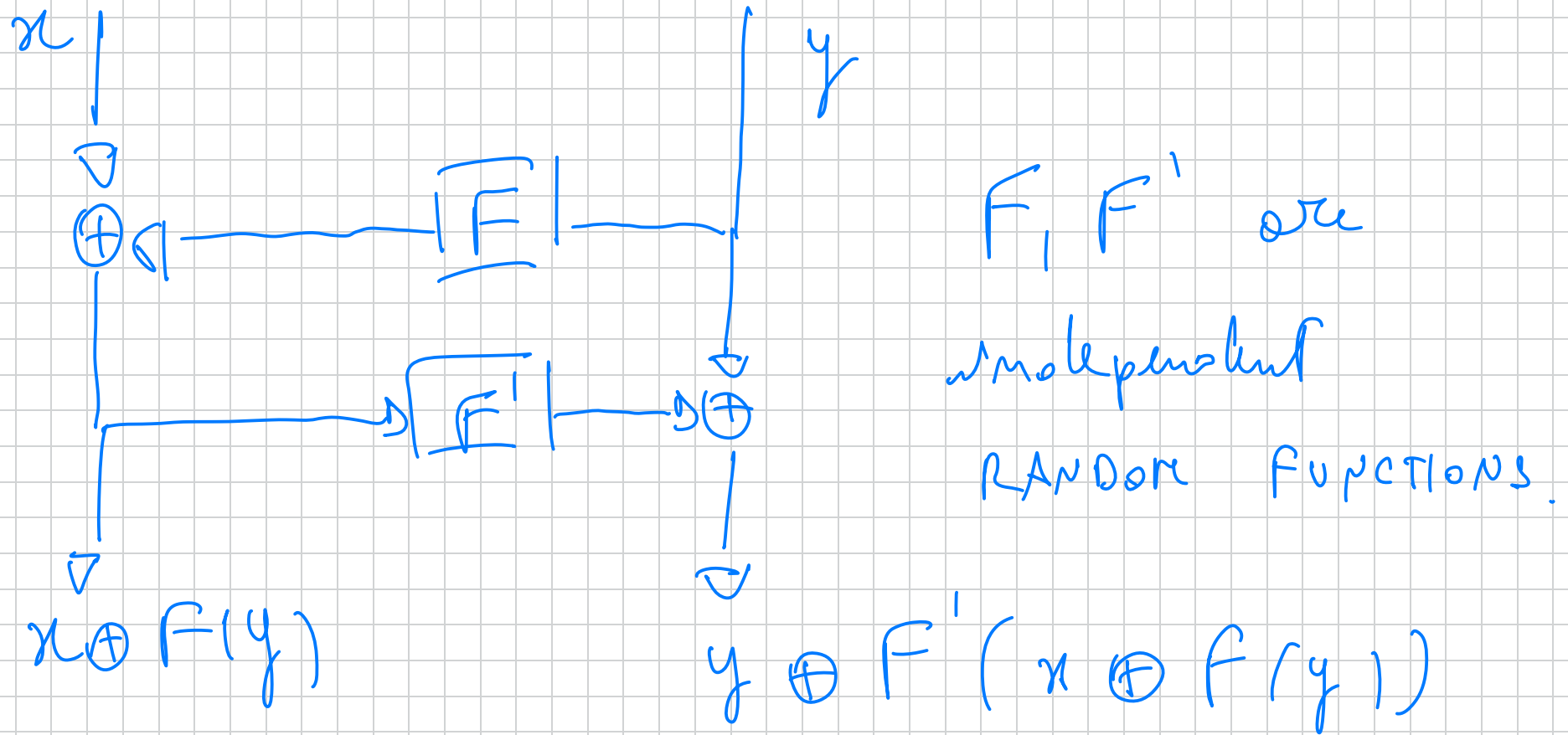
$$x' = y$$

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

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

Q: Is this a PRP (assuming F is a PRF)?
 No. Because 1st half of output =
 2nd half of input

Solution: Do not more Times.



Q: Is it a PRP now? No!

Observation: $\psi_{F, F'}(x, y) \oplus \psi_{F, F'}(x', y)$

$$= (x \oplus x' \mid \text{-----})$$

It turns out this is the "only" problem.

We can fix it by adding one more round!

In the real world: F is heuristic; all keys are derived from sample k (using PRG).

LEMMA For every UNBOUNDED attacker making $q = \text{poly}(\lambda)$ queries, the following are indistinguishable:

$$\rightarrow S : \mathcal{V}_{F, F'}(x, y) ; F, F' \leftarrow \mathcal{R}(n, n)$$

$$\neg) R : R(x, y) ; R \leftarrow R(2m, 2m)$$

so long as the queries made by A are
 "y-unique" (i.e. $y_i \neq y_j \forall i \neq j$).

Proof. Let H_n be the experiment where we
 reply to first n queries as from S , and
 all other from R . Now: $H_0 \equiv R$ and $H_q \equiv S$.
 Need to show $H_0 \approx_c H_q$.

Let us look at H_i (the first i queries):
 $(x_i \oplus F(y_i), y_i \oplus F'(x_i \oplus F(y_i))) ; i = 1, \dots, i-1$

$$x_n \oplus F(y_n), y_n \oplus F'(x_n \oplus F(y_n)), \dots$$

Since y_n is different from all y_i 's,

$F(y_n)$ is random and independent of $F(y_1), \dots, F(y_{n-1})$ and everything else.

So: $\left(\text{_____} \right)_{j=1, \dots, n-1}$ same as before

$$\left(x_i \oplus r, y_i \oplus F'(x_i \oplus r) \right)$$

for random r .

What's the probability that $x_N \oplus r = x_i \oplus F(y_i)$ for any of the $i = 1, \dots, N-1$

$$\Rightarrow \text{At most } (N-1) \cdot 2^{-M}$$

Assuming it does not happen:

$$\left(\underline{\hspace{10em}} \right); i = 1, \dots, N-1$$

$$\left(x_i \oplus r, y_i \oplus r' \right), \underline{\hspace{10em}}$$

r, r' RANDOM

By hybrid argument:

$$\begin{aligned} SD(S; R) &\leq \sum_n (n-1) 2^{-n} \leq q^2 \cdot 2^{-n} \\ &= \text{negl}(1). \end{aligned}$$

▀

THM. Assuming $\mathcal{F}$ is a PRF family, 3 rounds of $\mathcal{F}$ -based with independent keys is a PRP.

Proof: Consider the following systems.

$$\rightarrow T: \mathcal{F}_{K_3}(\mathcal{F}_{K_2}(\mathcal{F}_{K_1}(x, y)))$$

$$K_1, K_2, K_3 \leftarrow U_\lambda.$$

$$\rightarrow S : \mathcal{V}_{F, F'} (\mathcal{V}_{F''} (x, y))$$

$$\rightarrow R : R(x, y) ; R \leftarrow \mathcal{R}(2M, 2M)$$

$$\rightarrow P : P(x, y) ; P \leftarrow \mathcal{P}(2M, 2M)$$

RANDOM PERMUTATION.

1) $T \approx_c S$. Why? By the fact that F is a PRF.

2) $S \approx_S R$ for poly(1) queries.

Idea: a random gives you uniqueness!

$\mathcal{V}_{F||} (x_i, y_i)$ satisfies uniqueness.

Take any $(x_n, y_n) \neq (x_i, y_i)$. Two cases:

(N) $y_n = y_i$, then $x_n \neq x_i$

$$y_i'' = x_i \oplus F''(y_i)$$

$$= x_i \oplus F''(y_i)$$

$$\neq x_i \oplus F''(y_i) = y_i''$$

(NN) So, let $y_i \neq y_j$. Then, we would

$$\text{need: } x_i \oplus F''(y_i) = x_j \oplus F''(y_j)$$

$$\Leftrightarrow x_i \oplus x_j = F''(y_i) \oplus F''(y_j)$$

and this happens v.p. $\leq 2^{-M}$.

$$\Rightarrow \Pr[\tau \text{ fails}] \leq \binom{q}{2} \cdot 2^{-M} \\ = \text{negl}(\lambda).$$

Then, $S \approx R$ by the lemma.

3) $R \approx P$. A random function is already Stat. ind. from a random permutation answering $q = \text{poly}(\lambda)$ queries.



But one question remains: We can do SKE
building Shannon assuming any PRF (or F).

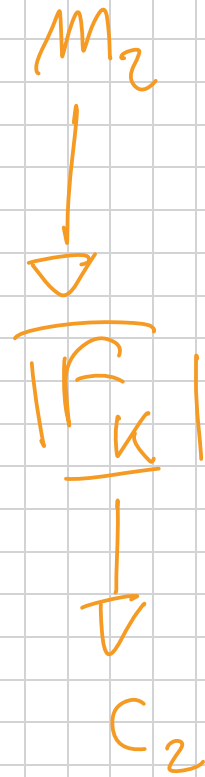
$$C = (r, F_k(r) \oplus m)$$

r RANDOM

What about very long $m = m_1, \dots, m_t$
 $m_i \in \{0, 1\}^M$. We need a so called

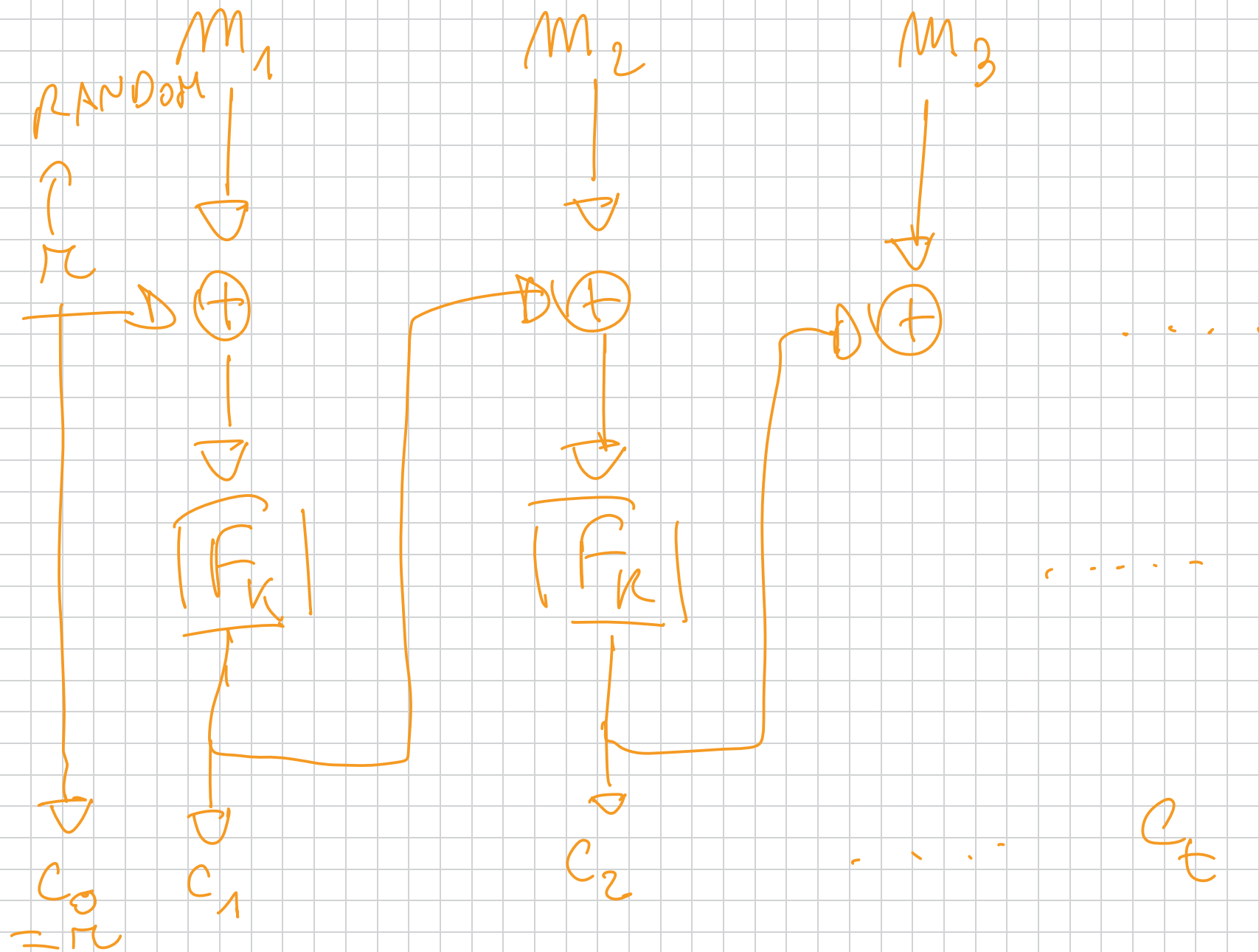
MODE of OPERATION. Sometimes also
DOMAIN EXTENSION.

Perhaps, the simplest case:

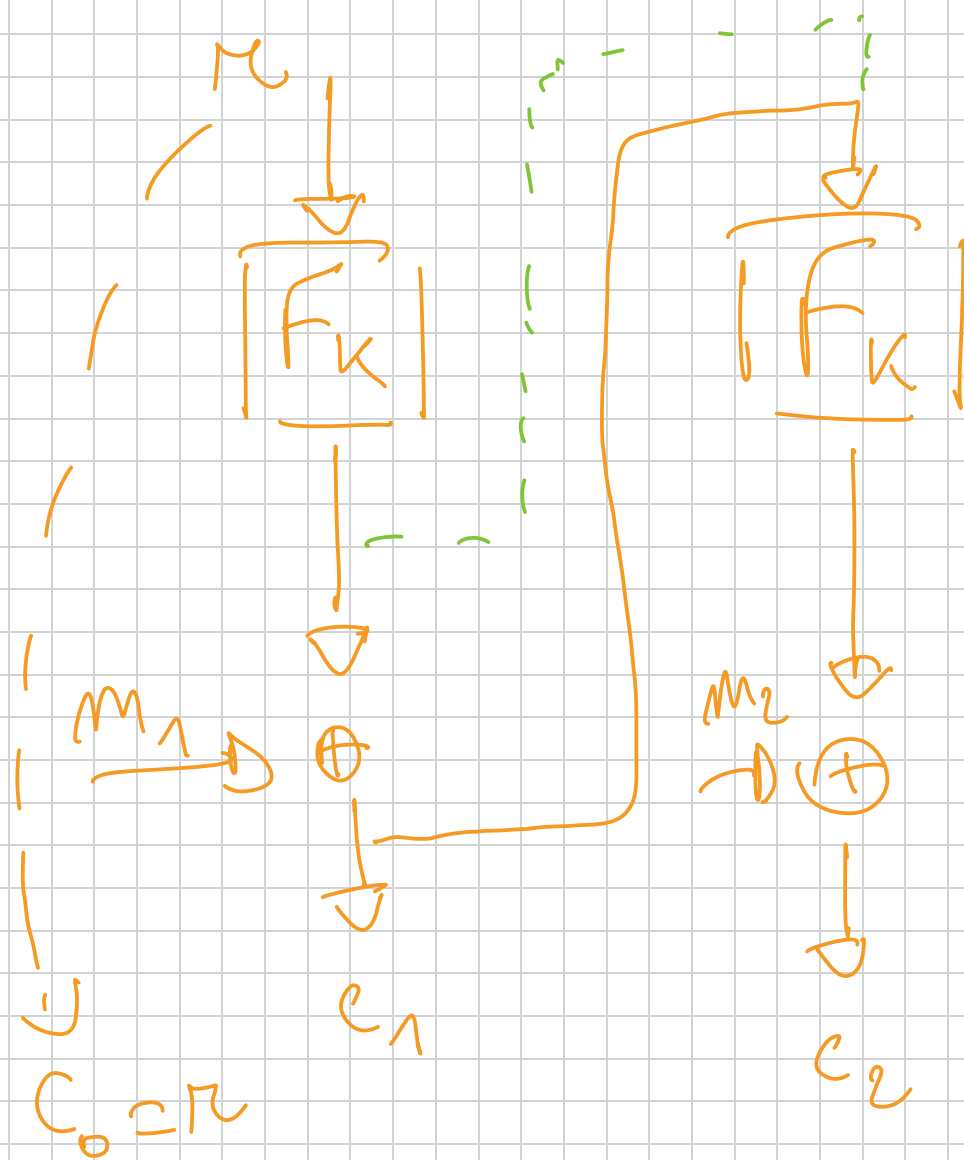


NEVER DO
THIS!

ECB



CBC

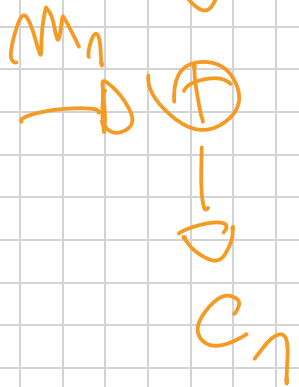
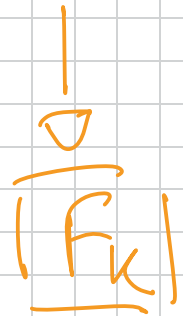


CFB
OFB

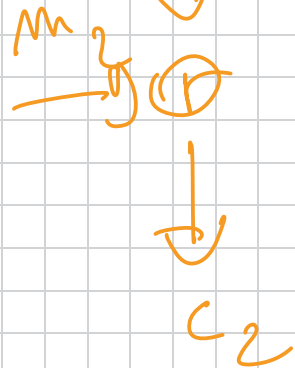
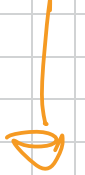
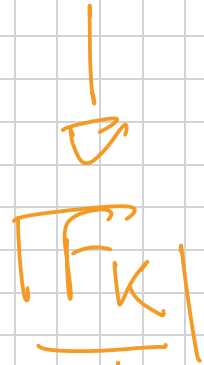
...

$\uparrow$ RANDOM OVER $\{0,1\}^m$

R

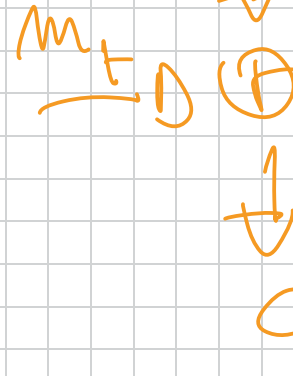


$R+1$



$+ \text{Mod } 2^m$
 $\dots$

$R+t-1$



CTR

$c_0 = R$

THM

CTR is

F is a PRF.

CPA-secure assuming

() for VARIABLE
INPUT

LENGTH.

Proof. Summar to our original proof for
single block.

A

$$m = m_1, \dots, m_t$$

$$c_0, c_1, \dots, c_t$$

C

$$m_0^* = m_{0,1}^*, \dots, m_{0,t}^*$$

$$m_1^* = m_{1,1}^*, \dots, m_{1,t}^*$$

$$c_0^*, c_1^*, \dots, c_t^*$$

$$m = m_1 \dots m_t$$

$$c_0, c_1, \dots, c_t$$

b'

Let G_0 be the above game with $b = 0$
and using CTR. Same for G_1 . We need
to show $G_0 \approx_c G_1$.

→ Thus means:

$$C_0 = \pi ; C_1 = F_K(\pi) \oplus M_1$$

$\vdots$

$$C_t = F_K(\pi + t - 1) \oplus M_t$$

By security of F , we can replace $F_K(\cdot)$
with $R \leftarrow R(n, n)$. Let us call this
 H_0, H_1 .

So, $G_0 \approx_c H_0$ and $G_1 \approx_c H_1$.

We finally introduce H_2 s.t. $c_0^*, c_1^*, \dots, c_t^*$

is uniformly random. We will show that

$H_0 \approx_s H_2$ and $H_1 \approx_s H_2$ assuming

queries is $q = \text{poly}(\lambda)$.

look at the challenge:

$$c_0^* = r^* \leftarrow U_m; \quad c_1^* = R(r^*) \oplus m_{b,1}^*$$

$\vdots$

$$c_t^* = R(r^* + t^* - 1) \oplus m_{b,t^*}^*$$

Let OVERLAP be the event that
 $\pi^*, \pi^*+1, \dots, \pi^*+t^*-1$ overlaps with
any of

$$\pi, \pi+1, \dots, \pi+t-1$$

If OVERLAP does not happen:

$$H_0 \equiv H_2 \equiv H_1$$

So, we only need to show:

$$P_\pi[\text{OVERLAP}] \leq \text{negl}(1).$$