

How do we build a PRF?

- From any OWF. Actually from ANY PRG. $\Leftarrow$ TODAY.

- Just believe that AES is a PRF.

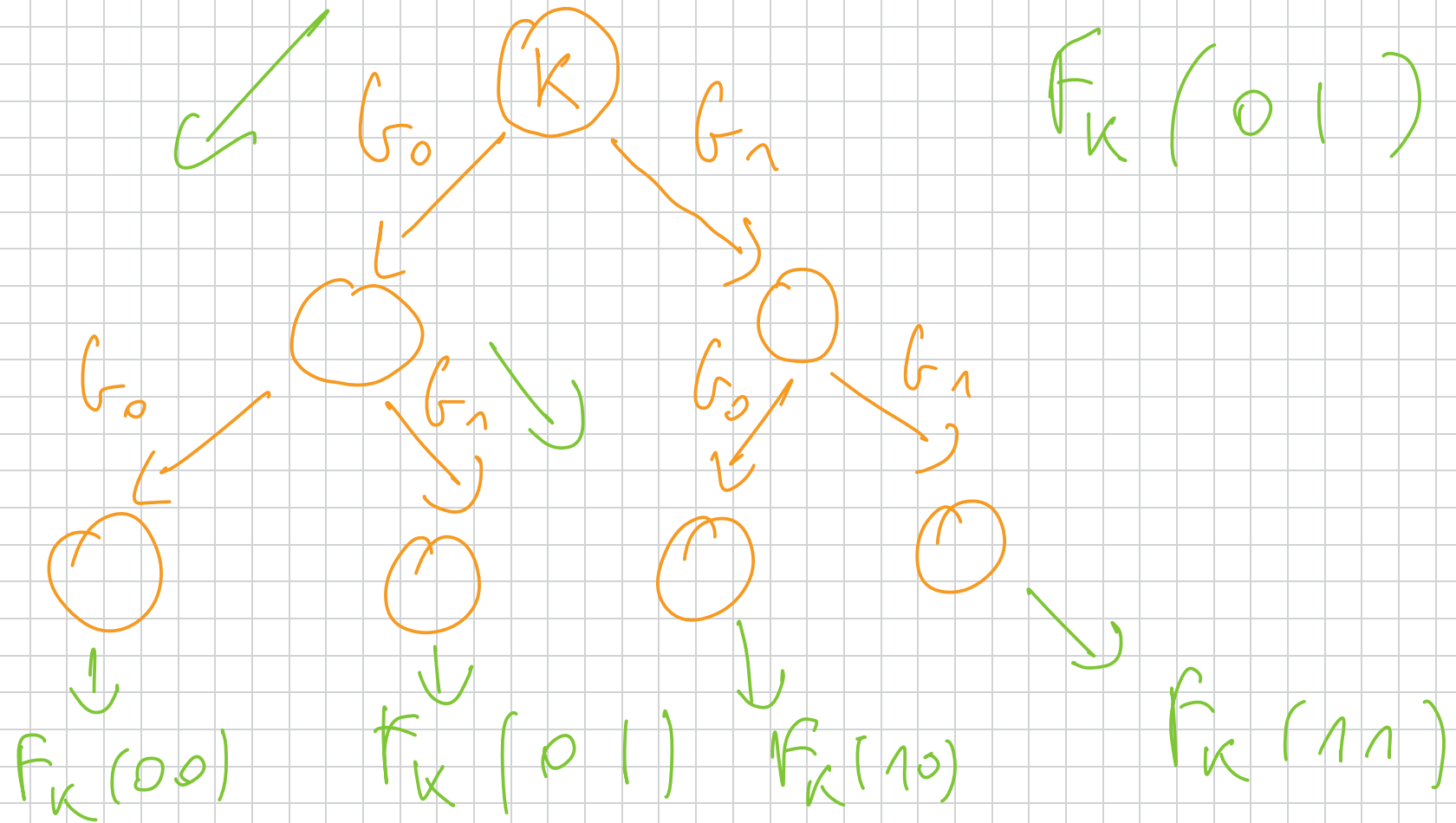
A famous construction: Goldreich, Goldwasser and Micali (GGM). It assumes:

$$G: \{0,1\}^l \rightarrow \{0,1\}^{2l}$$

We want to build $F_K: \{0,1\}^m \rightarrow \{0,1\}^l$

Think of $G(K) = (G_0(K), G_1(K))$ where

G_0, G_1 are the functions on splitting first / last 1 bits of $G(K)$.



$$F_k(x) = G_{x_m}(G_{x_{m-1}}(\dots G_{x_1}(x) \dots))$$

$$x = x_1 \dots x_m \in \{0,1\}^m$$

THM

A sampling G is a PRG, Then

$\mathcal{F} = \{F_k : \{0,1\}^m \rightarrow \{0,1\}^L\}$ is a PRF.

In the proof: Since k is random, $(G_0(k), G_1(k))$

$\approx_c (U_\lambda, U_\lambda)$ and then I could replace

all the keys with new random strings.

But this requires exp - many hybrids!

We will rely on a sample lemma:

LEMMA For any $t(\lambda) = \text{poly}(\lambda)$:

$$(G(k_1), \dots, G(k_t)) \stackrel{\sim}{\sim}_c (V_{2,1}, \dots, V_{2,t})$$

where $k_i \leftarrow U_\lambda \quad \forall i = 1, \dots, t.$

Proof. Hybrid argument:

$$H_0 \equiv (G(k_1), \dots, G(k_t))$$

$$H_1 \equiv (V_{2,1}, G(k_2), \dots, G(k_t))$$

$$U_{2,1}, U_{2,1}, G(K_3), \dots, G(K_e)$$

⋮

$$H_t \equiv (U_{2,1}, U_{2,1}, \dots, U_{2,1})$$

$$H_0 \sim_c H_1 \dots H_{t-1} \sim_c H_t \Rightarrow H_0 \sim_c H_t$$

$$H_0 \sim_c H_1$$

A

B

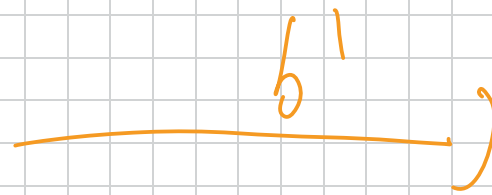
C

$$\leftarrow z_1, G(K_e), \dots, G(K_e)$$

$$\leftarrow z_1 \in \{0,1\}^{2,1}$$

$$\begin{array}{l} G(K_1) \\ z_1 \sim U_{2,1} \end{array}$$

$$K_2, K_3, \dots, K_e \in \mathcal{V}_1$$



let's prove The THM. By induction on $m(1) = \text{poly}(1)$. Let:

$$F'_k : \{0, 1\}^{m-1} \rightarrow \{0, 1\}^1$$

$$F_k : \{0, 1\}^m \rightarrow \{0, 1\}^1$$

$$F_k(x, y) = G_k(F'_k(y))$$

$$x \in \{0, 1\} \text{ and } y \in \{0, 1\}^{m-1}$$

By induction:

— GGM is secure for inputs of length $n = 1$. Because:

$$F_K(0) = G_0(K); F_K(1) = G_1(K)$$

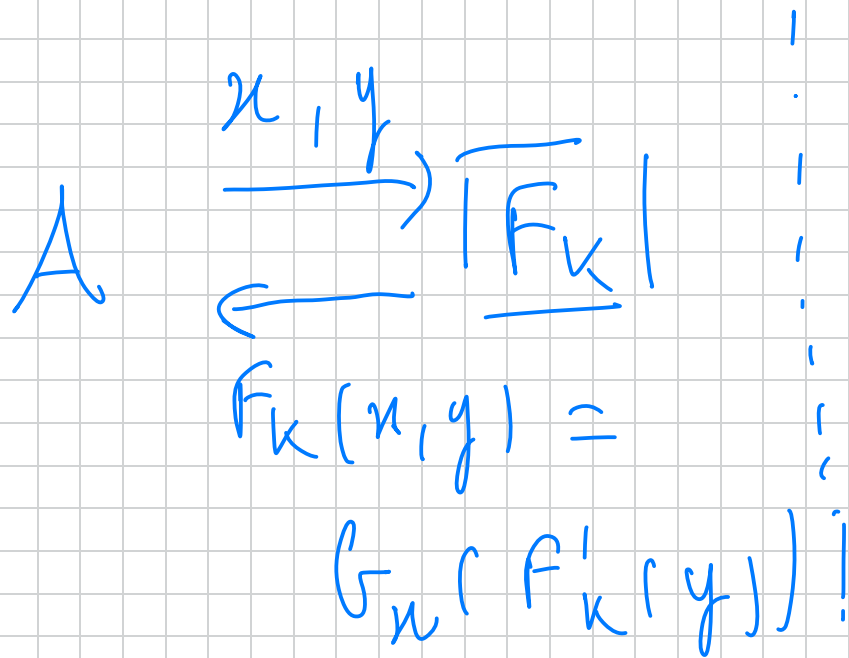
and $(G_0(K), G_1(K)) \stackrel{z}{\sim}_c (U_1, U_1)$

0	\$
1	\$

 $\stackrel{z}{\sim}_c$

0	$G_0(K)$
1	$G_1(K)$

- Assume F_k' is a PRF for $m-1$ input length. Then, we'll show F_k is also a PRF.



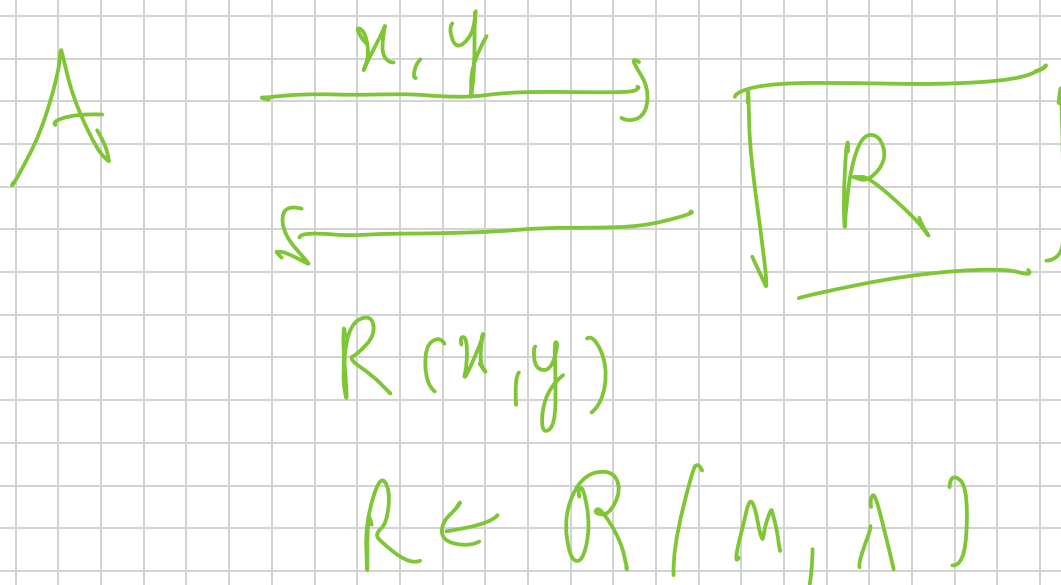
$\text{GAME}_0(\lambda)$



$$H(x, y) = G_k(R'(y))$$

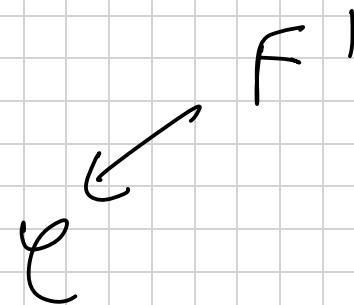
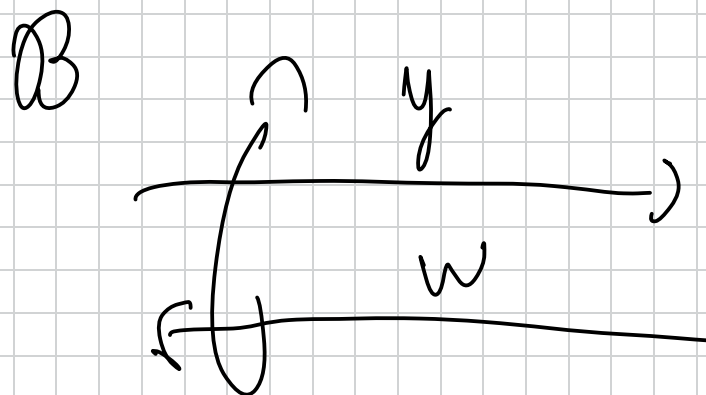
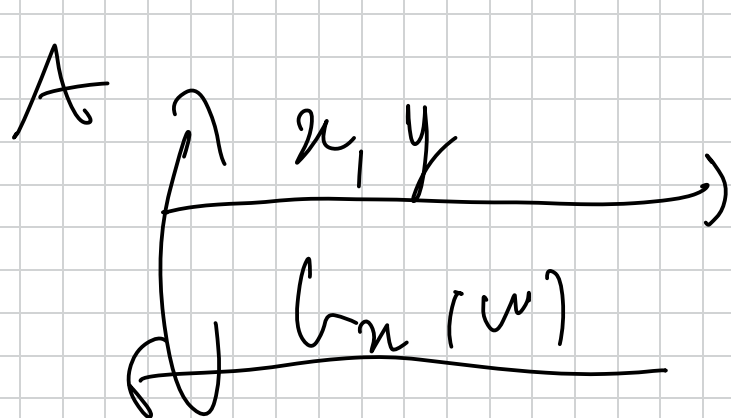
$$R' \leftarrow R(m-1, \lambda)$$

GAME, (λ)



Lemma $\text{GAME}_0(\lambda) \stackrel{\sim}{\sim}_c \text{GAME}_1(\lambda)$

Exercise: Reduction.



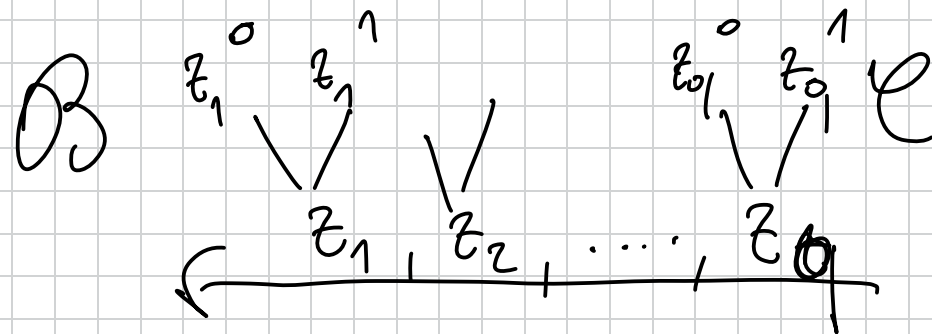
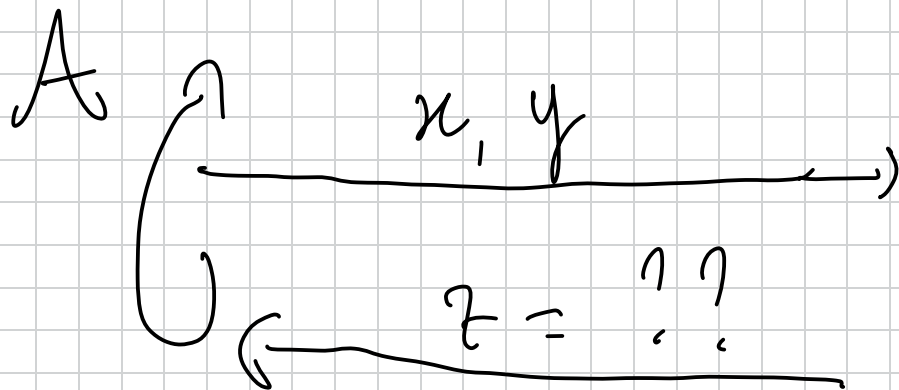
b^1

b^1

PERFECT!

LEMMA $\text{GAME}_1(A) \sim_c \text{GAME}_2(A)$.

By reduction T_0 on above lemma,



Let $t(\lambda) = q(\lambda) = \#$ queries made by A .
Define by $(z_i^0, z_i^1) = z_i$ the two
halves of each z_i (2,1 bits in total)

Now look: let x_1, y_1 be the first
query. Then, I can think of y_1 as fixing
the seed and reply with z_1^x . This
works.

Now, what about x_2, y_2 . Assume
 $y_2 \neq y_1$. Then, I'll do as before

2.1. reply $z_2^{n_2}$.

But what if instead $y_2 = y_1$.

Why $n_2 \neq n_1$. Now, I need to reply
with $z_1^{n_2}$ because in the yellow expres-

sion. we would run $G_{n_2}(R'(y_1))$ and

the set $R'(y_1)$ is the same for both
queries.

PM