1) PRG ⇒ PRF. GGM

; PRG $G(k) = (G_0(k), G_1(k))$

λ → λ + λ

First: Construct PRF with $n = 1$ -

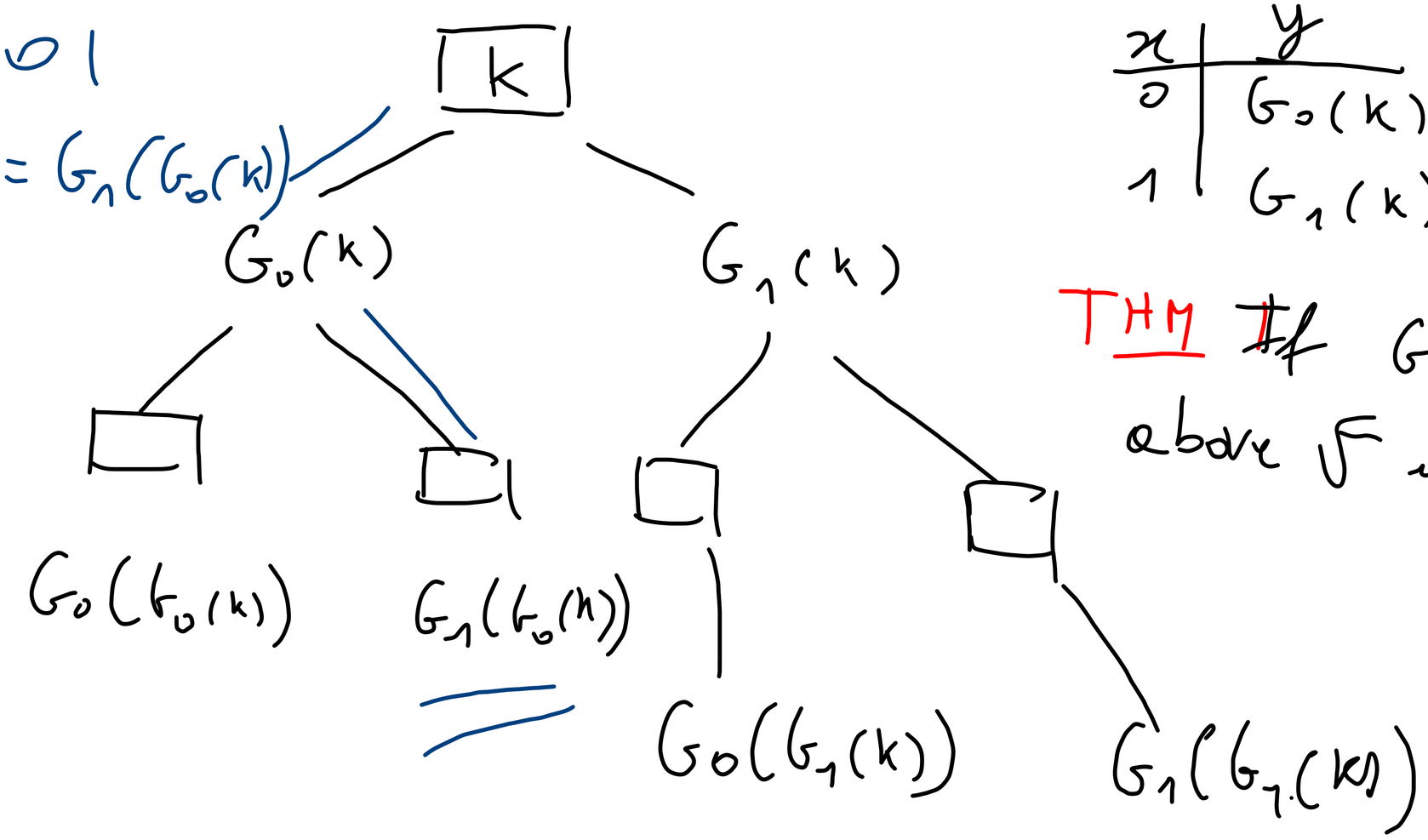
output $\ell = \lambda$

x	y
0	$G_0(k)$
1	$G_1(k)$

x	y
0	\$
1	\$

$x = 01$

$F_k(x) = G_1(G_0(k))$



THM If $G \in PRG$ above F is a PRF.

2) $Enc(k, m) = (r, F_k(r) \oplus m) = (c_0, c_1)$

$Dec(k, (c_0, c_1)) = F_k(c_0) \oplus c_1 = m.$ $\quad m \in \{0,1\}^n$

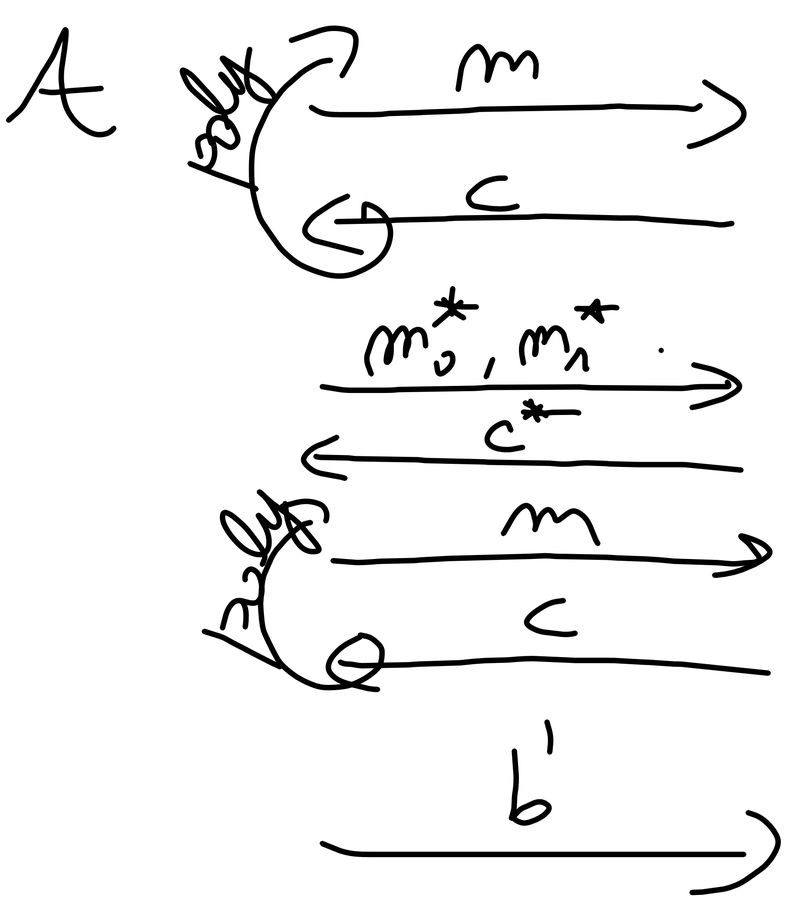
THM If F a PRF, above $\Pi = (Enc, Dec)$

is CPA-secure (for fixed-input length $n = n(\lambda)$).

$F = \{ F_k : \{0,1\}^n \to \{0,1\}^m \}_{k \in \{0,1\}^\lambda}$ F is

Proof. We need to show:

$\underline{\text{GAME}^{cpa}_{\Pi,A}(\lambda,b)}$ $\qquad$ $HYB(\lambda,b)$



C

$r \leftarrow\!\$ \{0,1\}^\lambda$ $\qquad$ $R \leftarrow\!\$ R(\lambda, m, n)$

$c = (r, F_k(r) \oplus m)$; $r \leftarrow\!\$ \{0,1\}^n$

$c^* = (r^*, F_k(r^* \oplus m_b^*))$; $r^* \leftarrow\!\$ \{0,1\}^n$

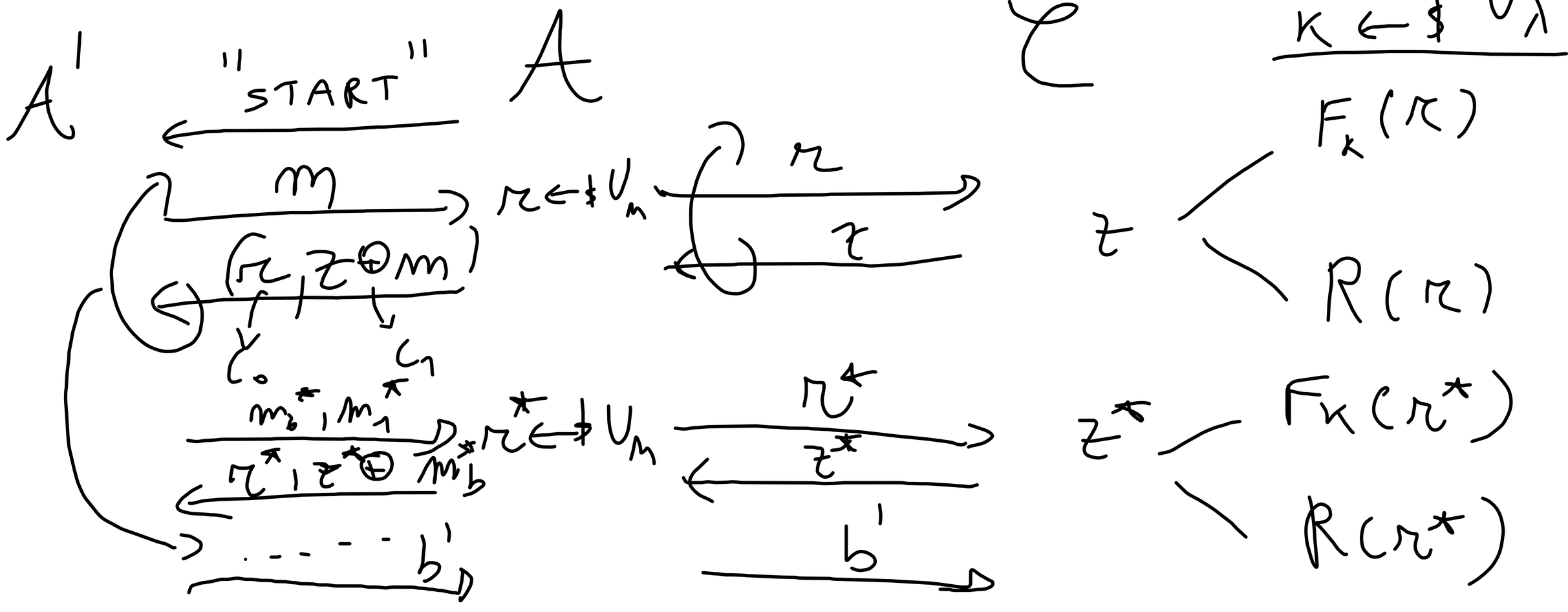
$c = (r, R(r) \oplus m)$

$c^* = (r^*, R(r^*) \oplus m_b^*)$

LEMMA. $\forall\, b \in \{0,1\}$: $GAME(\lambda, b) \tilde{\approx}_c HYB(\lambda, b)$.

Proof. By reduction to PRF security.

For $b \in \{0,1\}$, $\exists$ PPT A'



LEMMA $HYB(\lambda, 0) \approx_s HYB(\lambda, 1)$.

Proof. Defume BAD to be the event

$\exists\, i, j$ s.t. $r_i = r_j$ $\quad i, j \in [q]$ $\qquad q = \text{poly}$

# of queries.

The proof follows because:

(i) $Pr[BAD] \leq negl(\lambda)$

(ii) $HYB(\lambda, 0) \equiv HYB(\lambda, 1)$ conditioning on $\overline{BAD}$.

(ii) Follows because of $\overline{BAD}$, each CTX C, and also C^A is UNIFORM.

(i) $\Pr[BAD] = \Pr[\exists\, i, j \in [q] : i \neq j,\ r_i = r_j]$

$$\leq \sum_{i,j} \Pr[r_i = r_j]$$

$$= \sum_{i,j} Col(U_m)$$

$$= \binom{q}{2} \cdot 2^{-m} \leq poly(\lambda) \cdot 2^{-m} = negl(\lambda).$$

The statement follows because:

$$\left| \Pr[HYB(\lambda,0)=1] - \Pr[HYB(\lambda,1)=1] \right|$$

$$= \left| \Pr[HYB(\lambda,0)=1 \wedge BAD] + \Pr[HYB(\lambda,0)=1 \wedge \overline{BAD}] \right.$$
$$\left. - \Pr[HYB(\lambda,1)=1 \wedge BAD] - \Pr[HYB(\lambda,1)=1 \wedge \overline{BAD}] \right|$$

$$= \left| \Pr[HYB(\lambda,0)=1 \wedge BAD] - \Pr[HYB(\lambda,1)=1 \wedge BAD] \right|$$

$$= \Pr[BAD] \cdot \left| \Pr[HYB(\lambda,0)=1 \mid BAD] - \Pr[HYB(\lambda,1)=1 \mid BAD] \right|$$

$$\leq \Pr[BAD]$$

∎

Analysis: As we did in other proofs... ☒

Went:

$$\left| \Pr\left[b' = 1 : z_i = F_k(r_i);\ z^*_i = F_k(r^*) \right] \right.$$

$$\left. - \Pr\left[b' = 1 : z = R(r_i) \quad z^* = R(r^*) \right] \right|$$

$$\geq 1/\mathrm{poly}(\lambda) -$$