Recall the GGM construction:

$$G : \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$$

$$G(k) = \underbrace{(G_0(k)}_{\lambda \text{ bits}}, \underbrace{G_1(k))}_{\lambda \text{ bits}}$$

We build $\mathcal{F} = \{ F_k : \{0,1\}^{n(\lambda)} \to \{0,1\}^\lambda \}$ with $k \in \{0,1\}^\lambda$ such that

$$F_k(x) = G_{x_n}(G_{x_{n-1}}(\cdots G_{x_1}(k) \cdots))$$

For the proof, we use induction on $n(\lambda) = \text{poly}(\lambda)$. Let $F_K' : \{0,1\}^{n-1} \to \{0,1\}^{\lambda}$ and $F_K : \{0,1\}^{n} \to \{0,1\}^{\lambda}$ s.t.

$$F_K(x, y) = G_x(F_K'(y))$$

$$x \in \{0,1\}; \quad y \in \{0,1\}^{n-1}$$

LEMMA If $\{F_K'\}$ is a PRF, then $\{F_K\}$ is a PRF family.

We can use this lemma to prove security of GGM by induction.

In fact, for $n = 1$ GGM is:

$$F_k(x) \equiv G_x(k) \qquad x \in \{0,1\}.$$

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

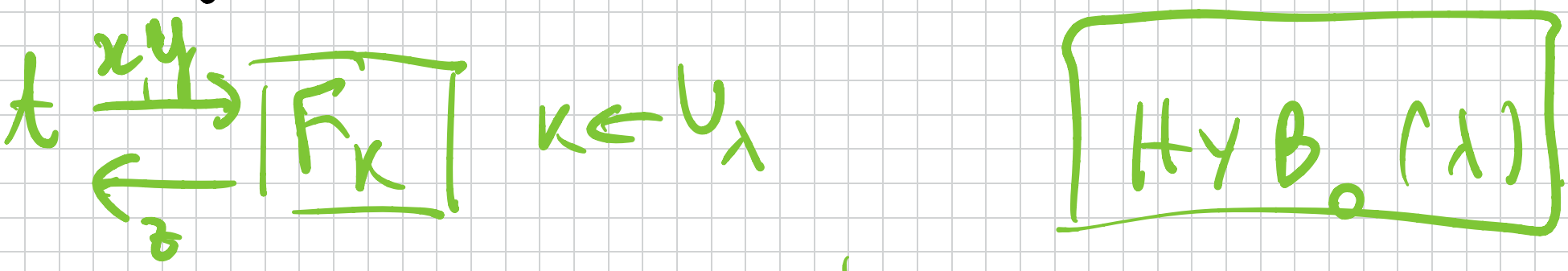
$\equiv_c$

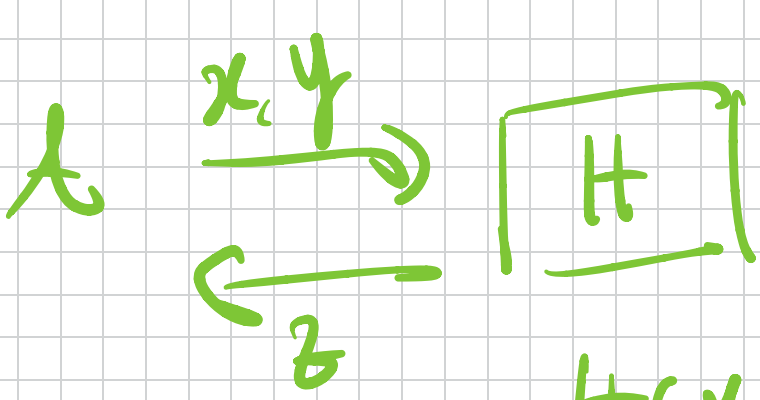
x	$R(x)$
0	\$
1	\$

because $(G_0(k), G_1(k)) \equiv_c U_{2\ell}$

For the induction step, take f_k' to be GGM construction on inputs of size $n-1$ and note that f_k is exactly GGM on inputs of size n.

Proof (of LEMMA). We consider:

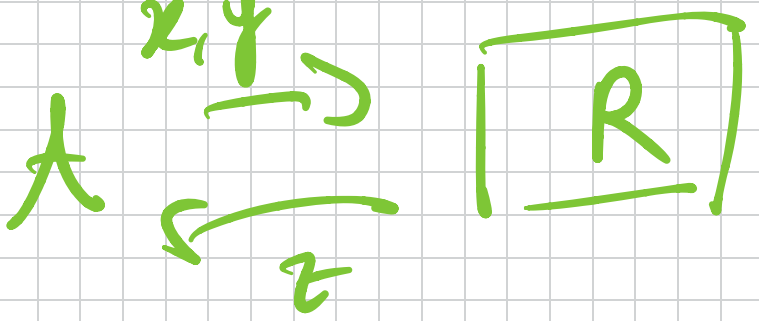




$R' \leftarrow OR(\lambda, u_{-1} \to \lambda)$

$HYB_1(\lambda)$

$H(x, y) = G_x(R'(y)) = z$



$R \leftarrow OR(\lambda, u \to \lambda)$

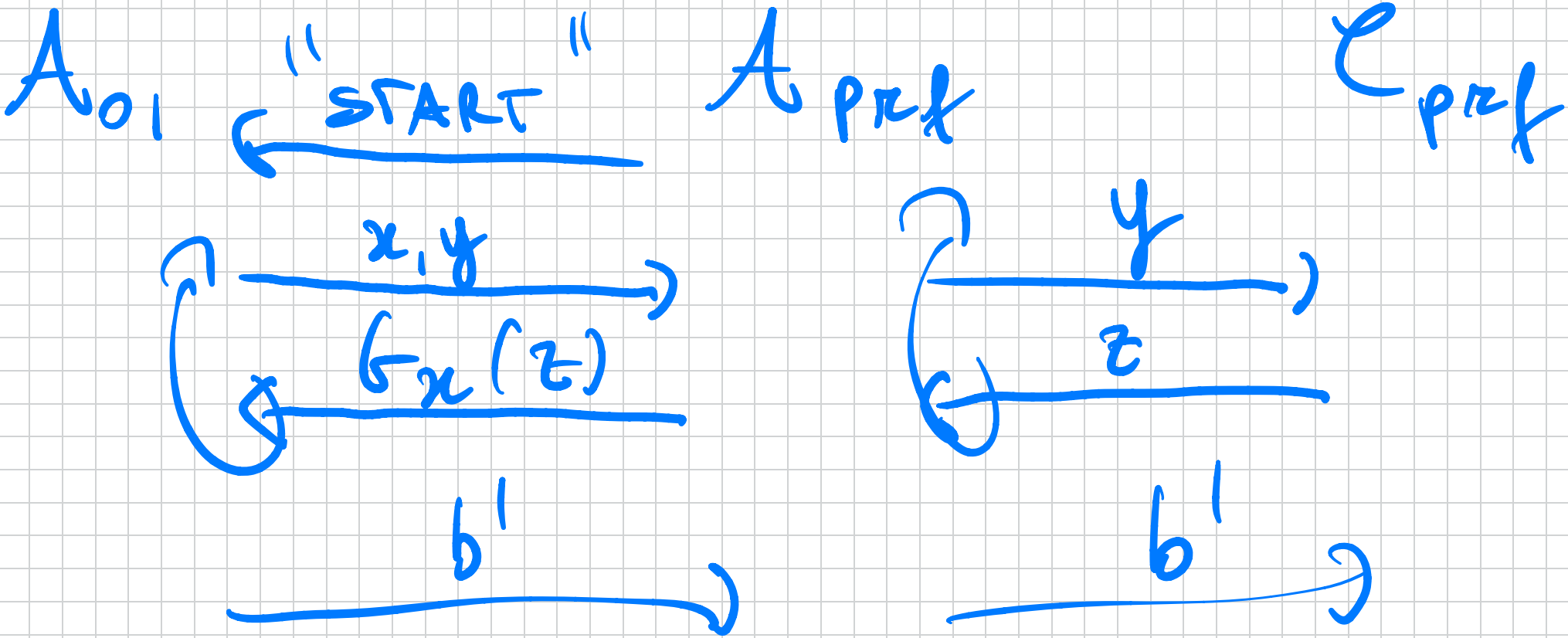
$HYB_2(\lambda)$

$z = R(x, y)$

Now, we first show $HYB_0(\lambda) \overset{c}{\approx} HYB_1(\lambda)$

This is true by reduction: Assume

$\exists$ PPT A_{01} Telling apart HYB_0 and HYB_1 w.p. $1/poly(\lambda)$. Build reduction A_{prf} against $\{F_k'\}$.



Look: If $z = f_k^{-1}(y)$, then

$G_x(z)$ is identical to what

A_0, receives in $B_0(\lambda)$.

On the other hand, if $z = R^{-1}(y)$ then

$G_x(z)$ is identical to what

A_0, receives in $B_1(\lambda)$.

Next, we prove $HYB_1(\lambda) \approx_c HYB_2(\lambda)$.

Here, we will use:

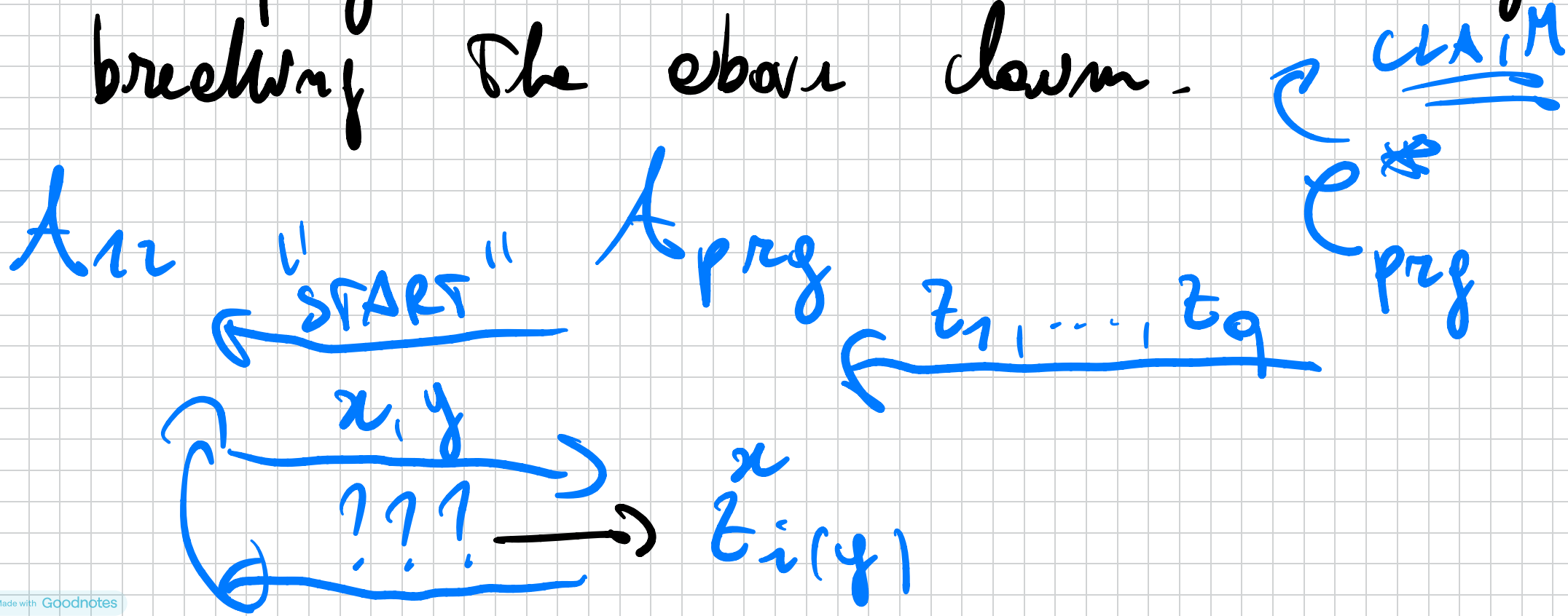
CLAIM If $G: \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$ is a PRG, then $\forall\, t(\lambda) = \text{poly}(\lambda)$:

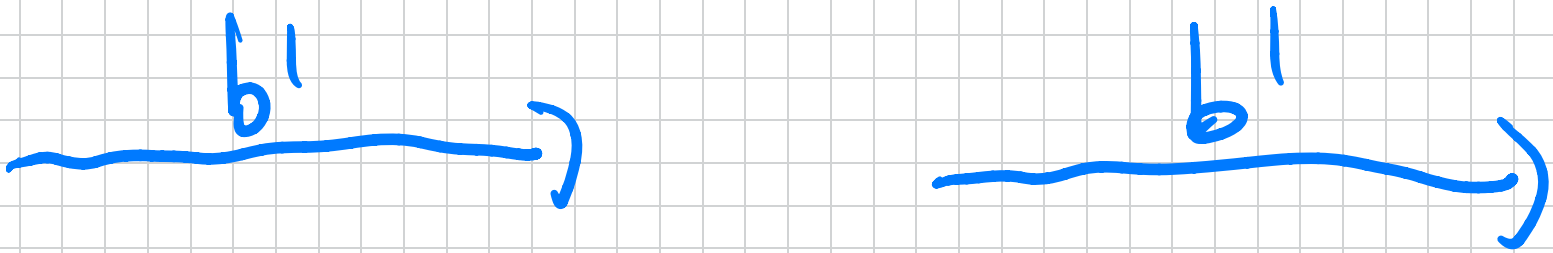
$$\left(G(k_1), \ldots, G(k_{t(\lambda)})\right) \approx_c$$

$$\left(U_{2\lambda}, \ldots, U_{2\lambda}\right) \equiv U_{2\lambda \cdot t(\lambda)}.$$

where $k_1, \ldots, k_t \leftarrow U_\lambda$.

Let's assume the claim true and make the reduction: $\exists$ PPT A_{12} telling apart $Hyb_1(\lambda)$ and $Hyb_2(\lambda)$ w.p. $\geq 1/poly(\lambda)$. We build PPT A_{prg} breaking the above claim.





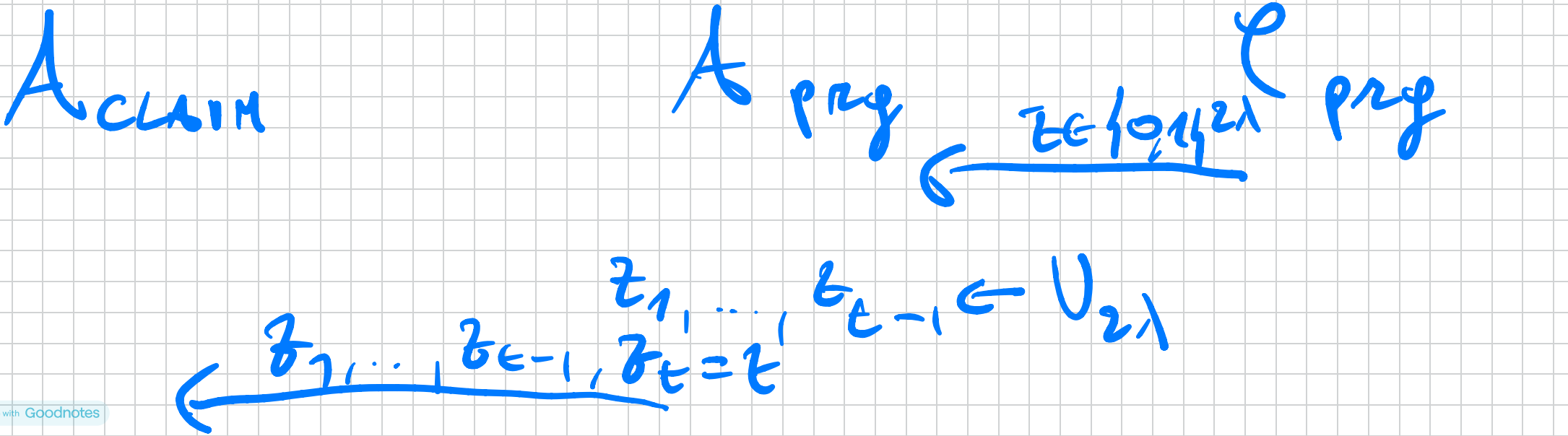
Let $t(\lambda) = q(\lambda) = \#$ queries made by A_{12}. Each of $z_i \in \{0,1\}^{2\lambda}$ and we can think of it as

$$z_i = (\underbrace{z_i^0}_{\lambda \text{ bits}}, \underbrace{z_i^1}_{\lambda \text{ bits}})$$

In the above reduction, $w(y)$ is the

index of the sample z_i that was used when t_{12} asked already for x, y. If it never asked, use the next available z_j. ∎

How to prove CLAIM ?! By reduction!



$\Rightarrow$ This only shows:

$$(U_{2\lambda_1}, \dots, U_{2\lambda}, G(K_t))$$

$$\simeq_c (U_{2\lambda_1}, \dots, U_{2\lambda}, O_{2\lambda})$$

This is basically 1st hybrid

2nd hybrid:

$$(U_{2\lambda_1}, \dots, U_{2\lambda}, G(K_{t-1}), G(K_t))$$

$$\left(v_{2\lambda_1}, \ldots, v_{2\lambda_l}, v_{2\lambda}, \sigma(k_t) \right)$$