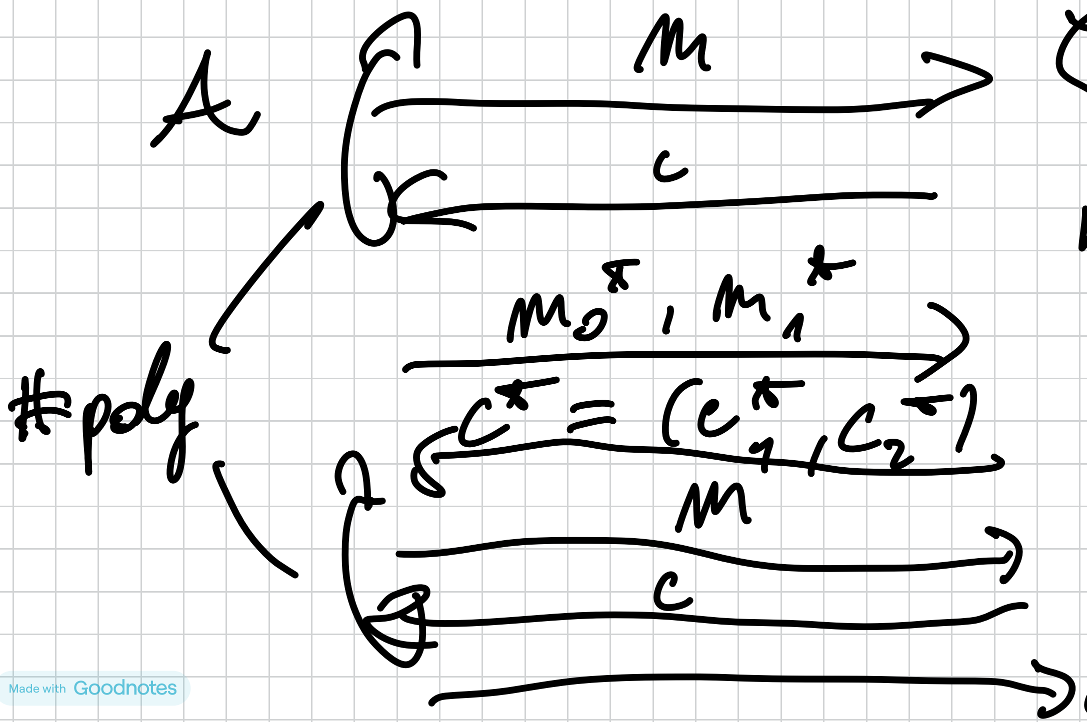
DEF (UFCMA) Tag is UFCMA iff $\forall$ PPT A : $\Pr[\mathrm{GAME}^{ufcma}_{A,Tag}(\lambda) = 1] \leq negl(\lambda)$.

THM 2 Assuming F a PRF, $Tag(K,m) = F(K,m)$ is UFCMA for FIL.

Proof (THM 1). Start with CPA game:



$\mathcal{C}_{cpa}$ $\quad G(\lambda, b)$ $\quad H(\lambda, b)$

$K \leftarrow \{0,1\}^\lambda$ $\quad$ Pick R

$c = (c_1, c_2)$

$c_1 = r \leftarrow \{0,1\}^n$

$c_2 = F_K(r) \oplus m$ $\quad R(r) \oplus m$

$c_1^* = r^* \leftarrow \{0,1\}^n$

$$c_2^* = F_K(r^*) \oplus m_b^*$$

$$R(r^*) \oplus m_b^*$$

We need to show: $\forall$ PPT A:

$$|\Pr[G(\lambda,0)=1] - \Pr[G(\lambda,1)=1]| \leq negl(\lambda).$$

Move to "mental" experiment $H(\lambda, b)$, where we replace $F_K(\cdot)$ with function $R: \{0,1\}^n \to \{0,1\}^n$ chosen randomly among all possible functions.

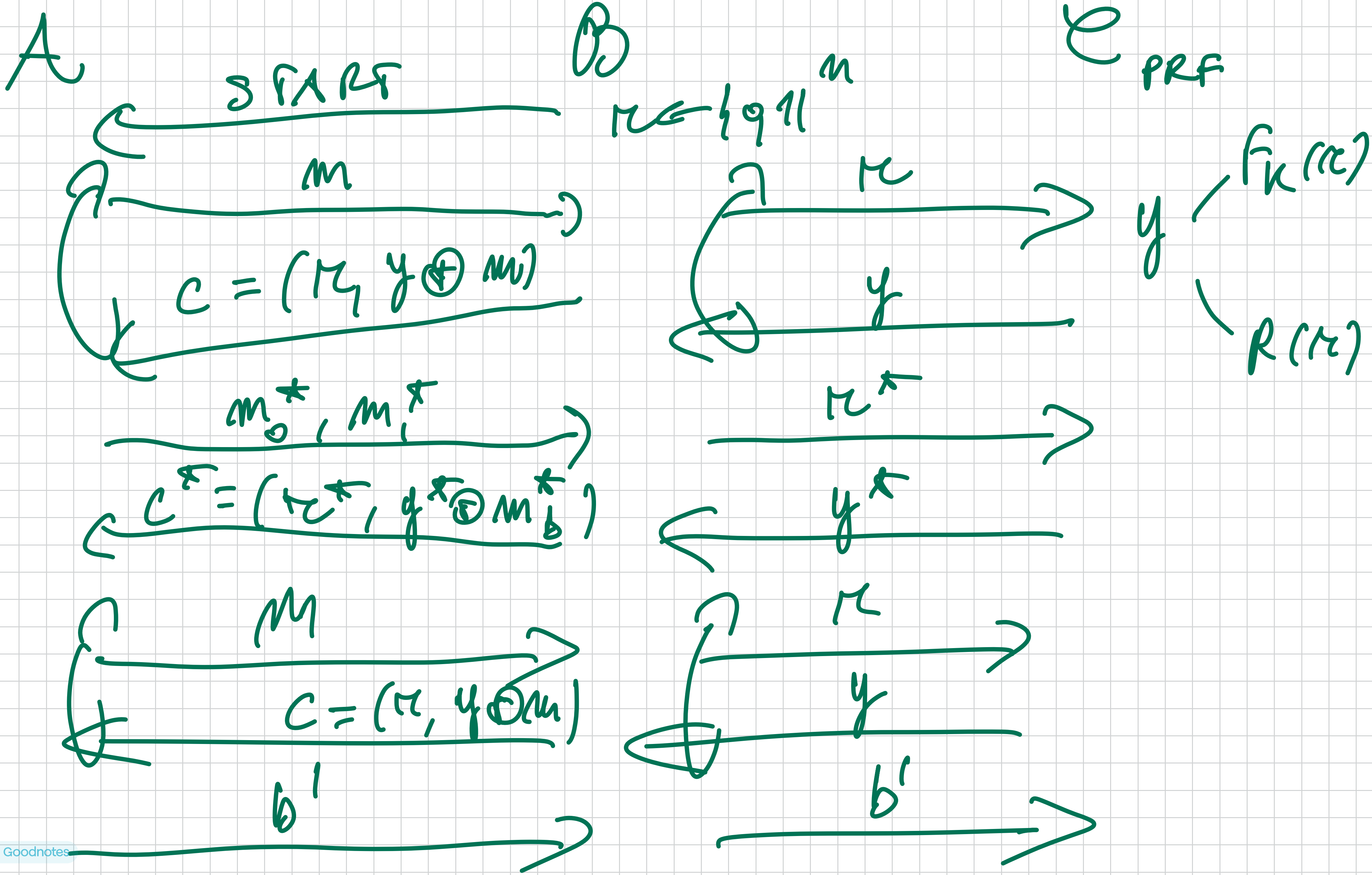
LEMMA. For every $b \in \{0,1\}$, $H(\lambda,b) \approx_c G(\lambda,b)$.

DIM. By reduction to security of PRF. Fix b.

Assume not: $\exists$ PPT A s.t.

$$|\Pr[G(\lambda,b)=1] - \Pr[H(\lambda,b)=1]| \geq 1/poly(\lambda)$$

Build PPT $\mathcal{B}$ against F :



Analysis: By inspection B makes a perfect simulation of A's view.

$$\Pr[G(\lambda, b) = 1] = \Pr[\mathrm{REAL}(\lambda) = 1]$$

$$\Pr[H(\lambda, b) = 1] = \Pr[\mathrm{RAND}(\lambda) = 1] \quad \boxtimes$$

Let $H'(\lambda, b)$ be s.t. we answer all queries with UNIFORM (c_1, c_2) and also (c_1^*, c_2^*) is UNIFORM. Clearly:

as long as $\# \text{ctxs} = \text{poly}(\lambda)$ $\quad H'(\lambda, 0) \equiv H'(\lambda, 1)$.

LEMMA $H(\lambda, b) \approx_s H'(\lambda, b) \quad \forall\, b \in \{0, 1\}$.

Proof. → Poundland Technique: Say that A

and B are identical unless some BAD EVENT E happens. Then:

$$SD(A;B) \leq \Pr[E].$$

The BAD EVENT: We want that all the r's are DISTINCT; if they are then (c_1, c_2) in $H(\lambda, b)$ is UNIFORM and also (c_1^*, c_2^*). E is the event that they collide:

$$\Pr[\exists\, i,j : r_i = r_j ;\ r_i, r_j \in \{0,1\}^n]$$

$$\leq \sum_{j,i} \underbrace{\Pr[r_j = r_i]}_{Col(U_M) = 2^{-M}} \qquad \text{UNION BOUND}$$

$$= \binom{q}{2} \cdot 2^{-M} \leq \underbrace{q^2}_{poly(\lambda)} \cdot \overbrace{2^{-M}}^{negl(\lambda)} = negl(\lambda)$$

where q is the # of ctxs.

$\hookrightarrow$ $q = poly(\lambda)$.

$$\Rightarrow G(\lambda, 0) \approx_c H(\lambda, 0) \approx_s H'(\lambda, 0) \equiv H'(\lambda, 1)$$

$$\approx_s H(\lambda, 1) \approx_c G(\lambda, 1) \quad \blacksquare$$

Proof (Thm. 2). We need to assume that $n = n(\lambda) = \omega(\log \lambda)$ super-logarithmic in λ.

$G(\lambda)$

A		Challenger
	$\xrightarrow{\quad m \quad}$	$k \leftarrow \{0,1\}^\lambda$
	$\xleftarrow{\quad \tau \quad}$	$\tau = F_k(m)$
	$\xrightarrow{\quad m^*, \tau^* \quad}$	Output 1 iff $F_k(m^*) = \tau^*$, $m^* \notin \{m\}$.

$\forall$ PPT A: $\Pr[G(\lambda) = 1] \leq \mathrm{negl}(\lambda)$.

Let $H(\lambda)$ be same as $G(\lambda)$ but with random table $R : \{0,1\}^n \to \{0,1\}^n$. So

$$\tau = R(m)$$

and A wins iff $\tau^* = R(m^*)$ and m^* FRESH.

LEMMA $\forall$ PPT A:

$$\left| \Pr[G(\lambda)=1] - \Pr[H(\lambda)=1] \right| \leq negl(\lambda)$$

Dim. By reduction:

$A \xleftarrow{\text{START}} B \qquad C_{PRF}$

$\xrightarrow{m}$ $\quad$ $\xrightarrow{m}$

$\xleftarrow{\tau}$ $\quad$ $\xleftarrow{\tau}$

$\xrightarrow{(m^*, \tau^*)}$ $\quad$ $\xrightarrow{m^*}$

$\xleftarrow{\tilde{\tau}}$

If $\tilde{\tau} = \tau^*$

$b' = 1$

$\xrightarrow{b'}$

Else $b' = 0$

By inspection :

- $\Pr[\, REAL(\lambda) = 1 \,] = \Pr[\, G(\lambda) = 1 \,]$
- $\Pr[\, RAND(\lambda) = 1 \,] = \Pr[\, H(\lambda) = 1 \,]$

$\Rightarrow \Leftarrow$ $\blacksquare$

LEMMA $\Pr[\, H(\lambda) = 1 \,] \leq negl(\lambda)$

$\forall$ UNBOUNDED A

(as long as $n = \omega(\log \lambda)$).

Proof. Only way to forge in $H(\lambda)$ is to guess the output of $R(m^*)$ on a fresh input m^*. Since this is uniform:

$$\Pr[\, H(\lambda) = 1 \,] \leq 2^{-\mu} = negl(\lambda)$$

because $\mu = \omega(\log \lambda)$. $\blacksquare$

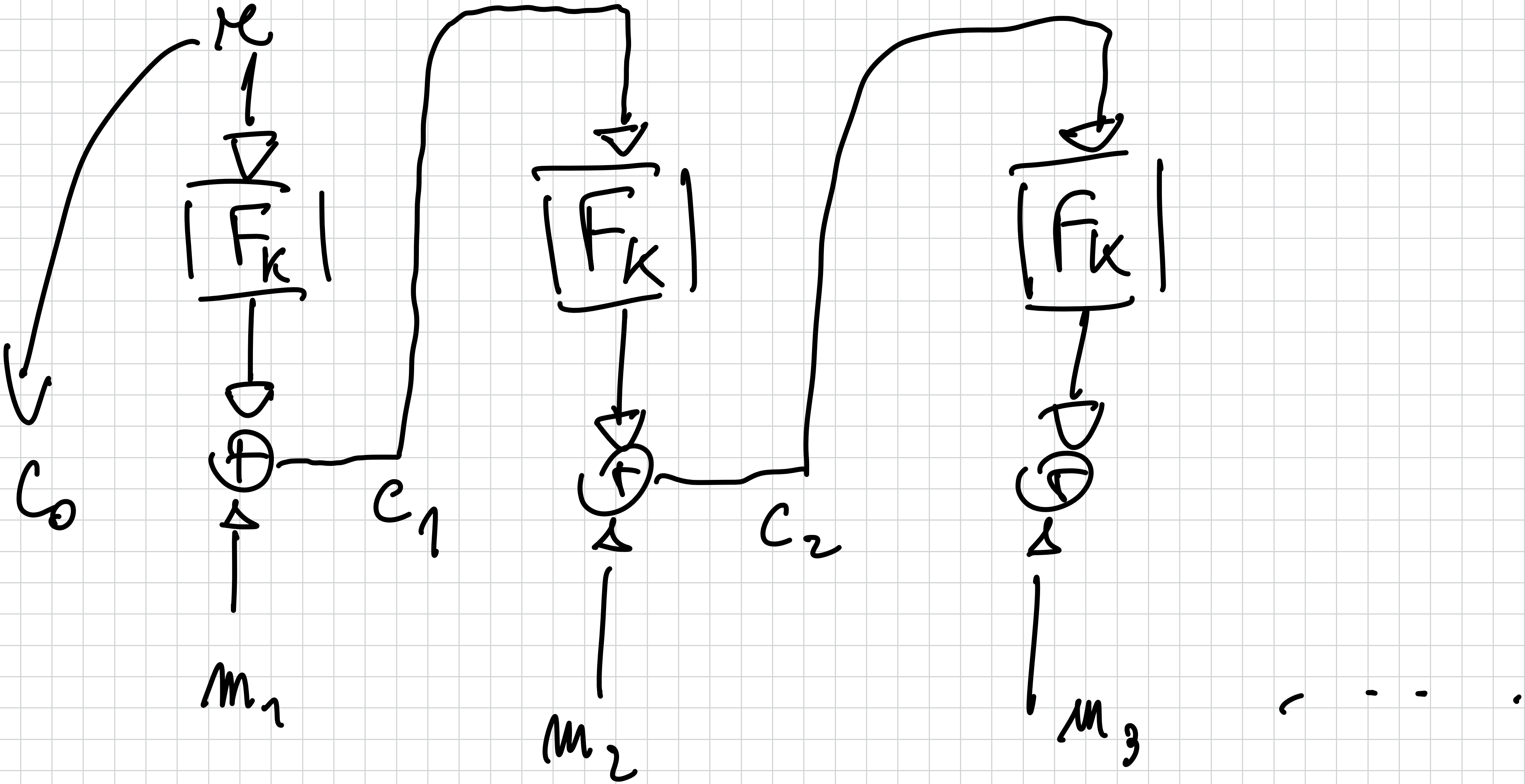
Next step: 1) How to go from FIL to VIL?
2) How to combine encryption and authentication.

Let's start with 1) for SKE. These are the so-called MODES OF OPERATION.

<u>CFB</u> (Cipher Feedback mode)

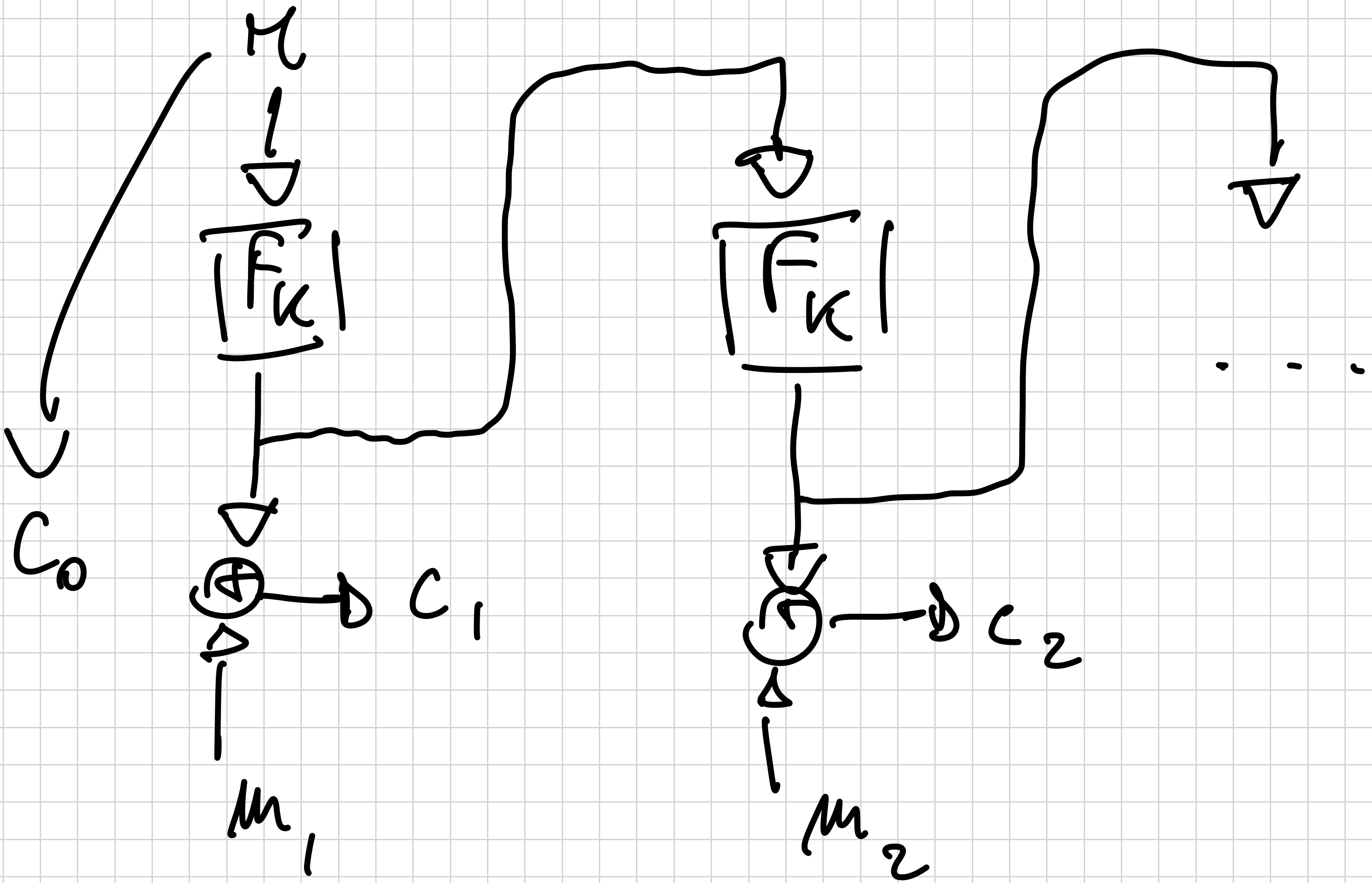
Let $m = m_1 \| m_2 \| m_3 \ldots$

$$m_i \in \{0,1\}^n$$

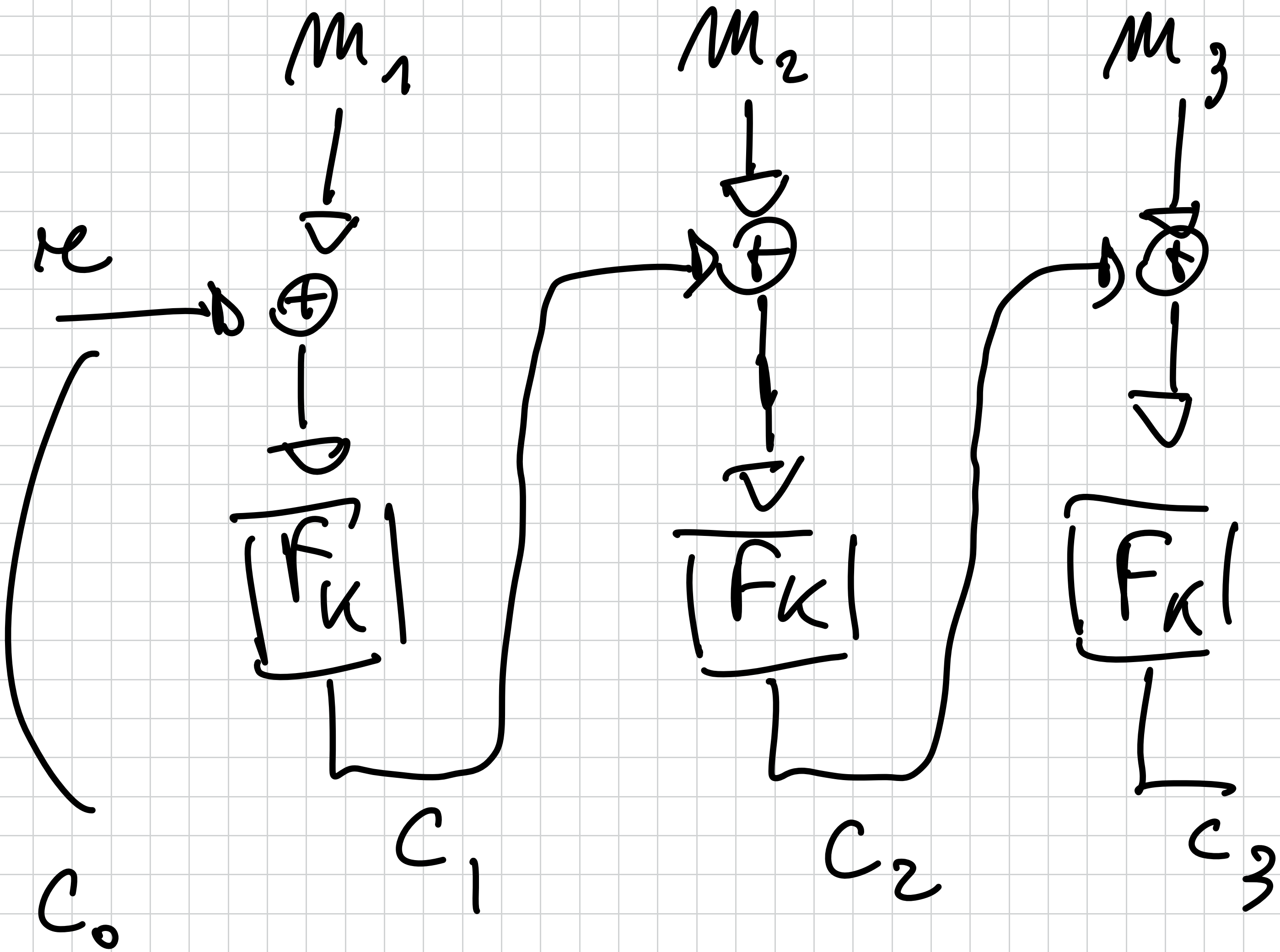


$$c = (c_0, c_1, c_2, c_3, \dots)$$

OFB (Output Feedback).



CBC (Cipher Block Chaining).



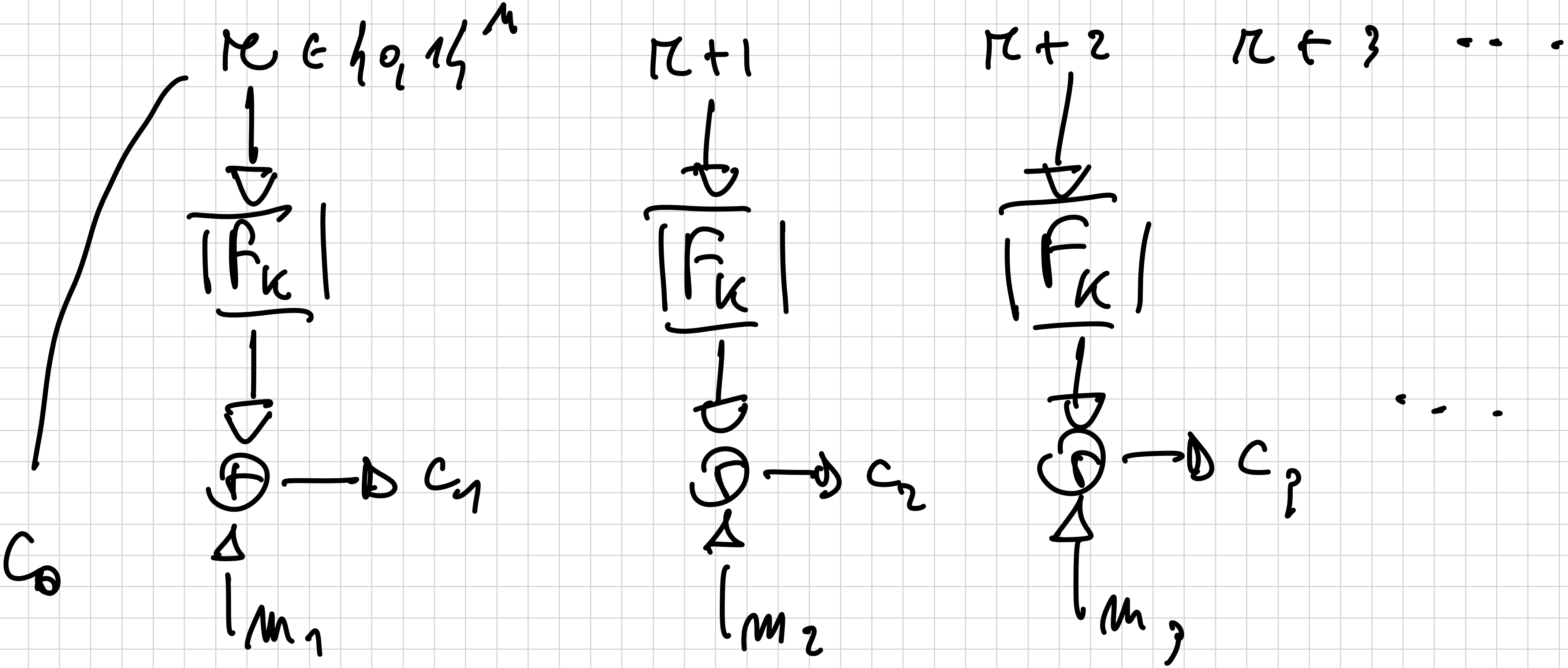
F must be a PRP (PERMUTATION)

To decrypt: need to evaluate $F_K^{-1}(\cdot)$

PRP: We'll discuss it later. In practice AES is a PRP.

In Theory: OWF $\Rightarrow$ PRGs $\Rightarrow$ PRFs $\Rightarrow$ PRPs.

<u>CTR</u> (Counter mode)



r is an integer mod 2^n and addition is also mod 2^n.

Thm. If F a PRF then CTR mode is CPA secure for VIL.