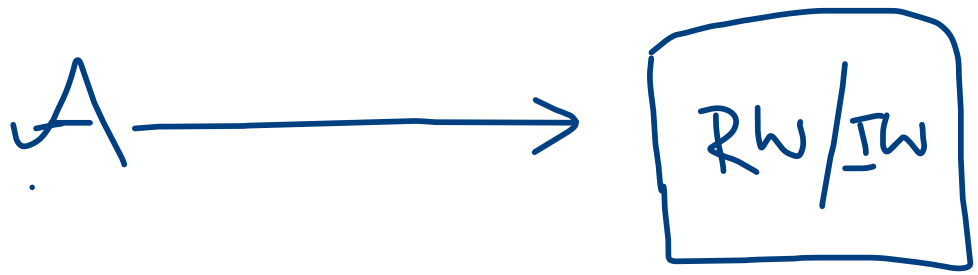
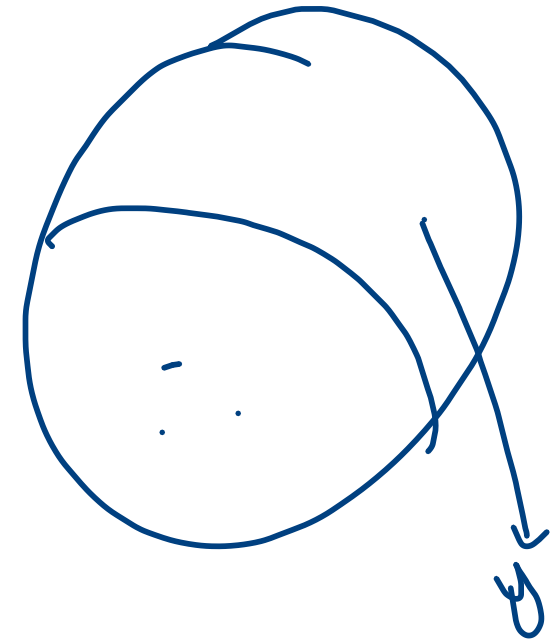
1. Random Oracle model ⟵ Hash fn

2. Ideal Cipher Model. ⟵ Block cipher

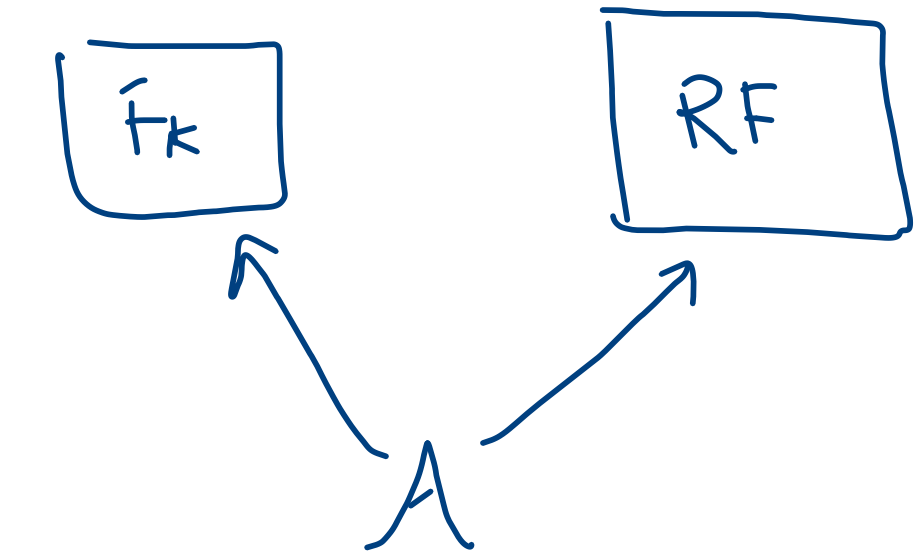
$$P(RF(x)=y \mid RF(x_1)=y_1 \cdots RF(x_q)=y_q) = \frac{1}{N} \qquad N = |\text{Range}|$$

$x \notin x_1, \ldots, x_q \quad \forall y$

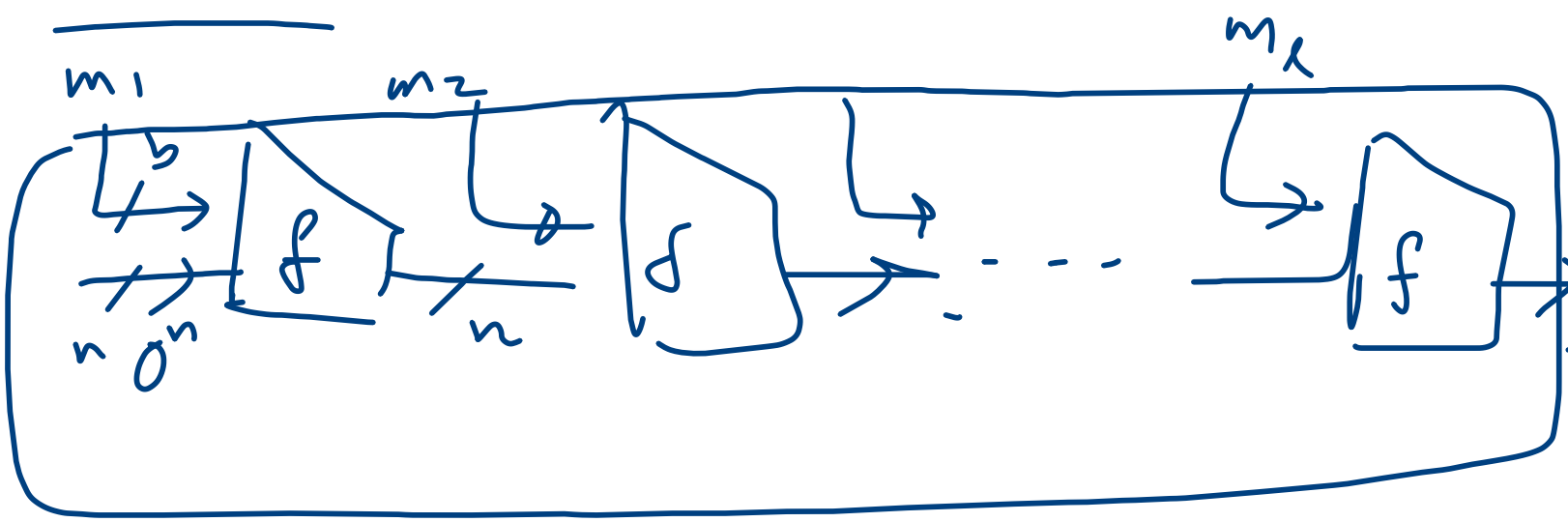


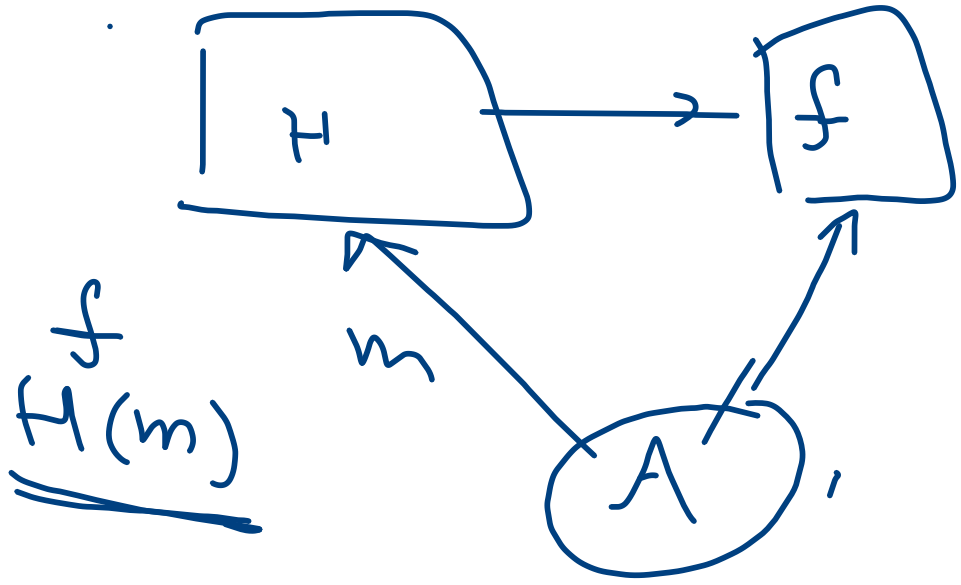


PRF



Hash





Manner

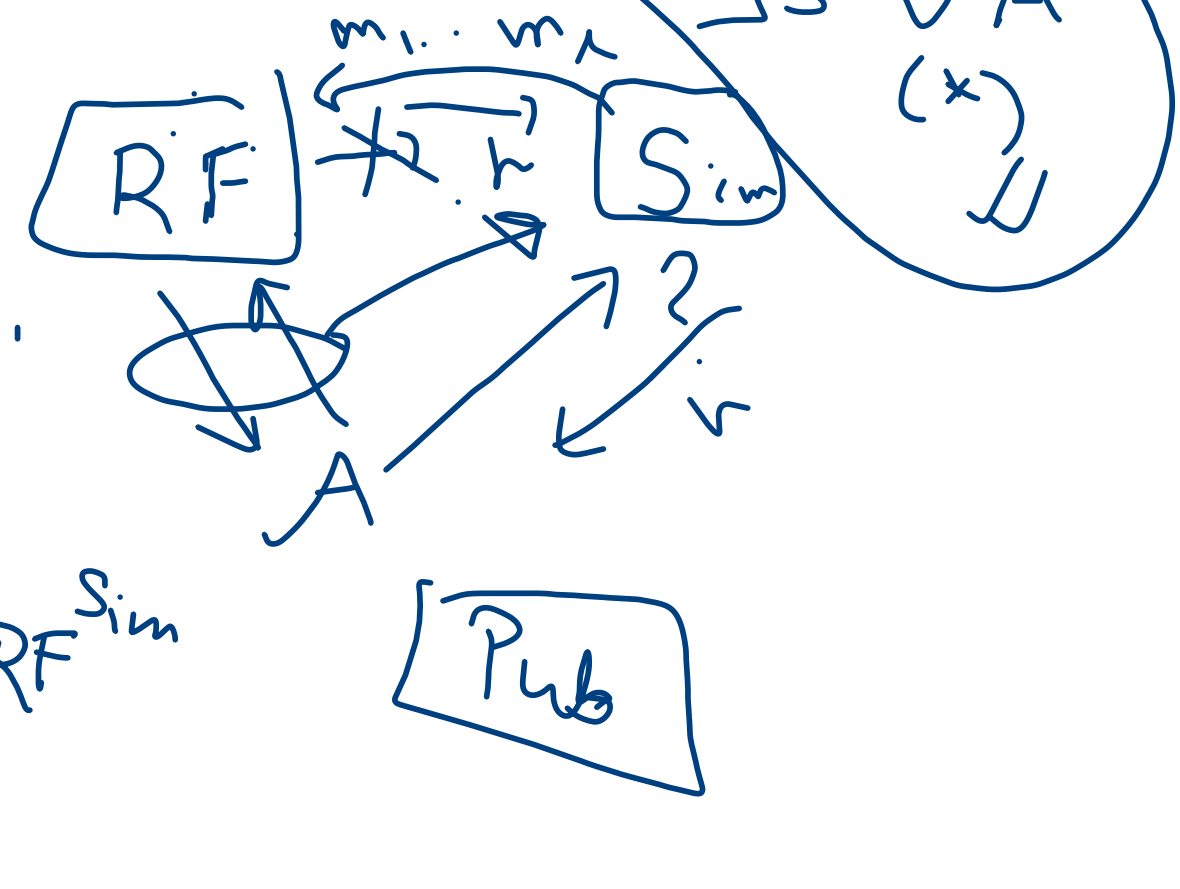
$\forall A \; \exists S$

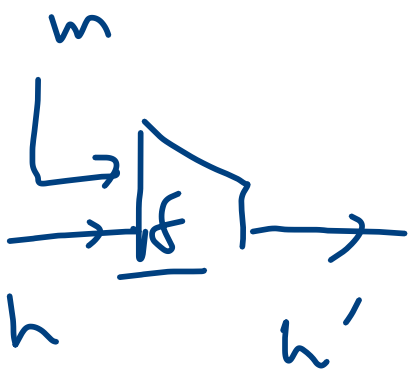
$\left(H^f, f\right) \approx \left(R, S^R\right)$ - (*)

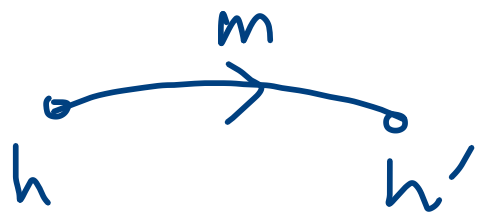
Coron et al.

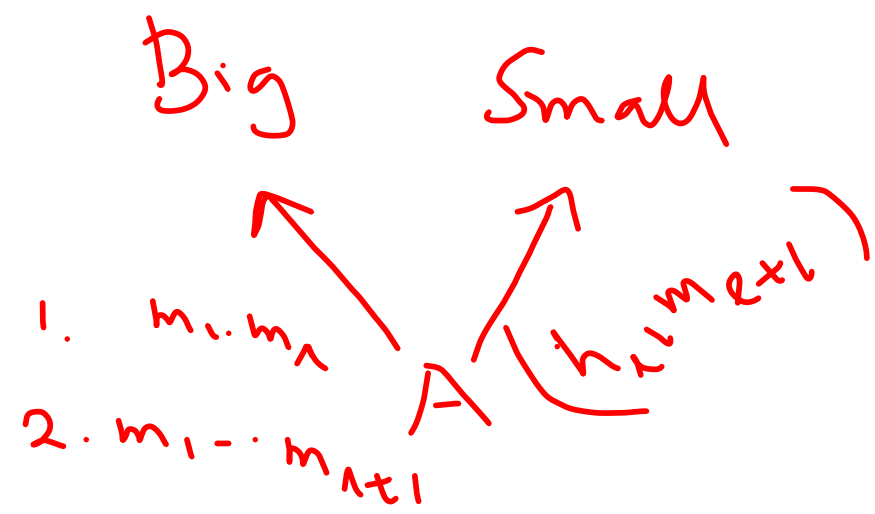
$\exists S \; \forall A$

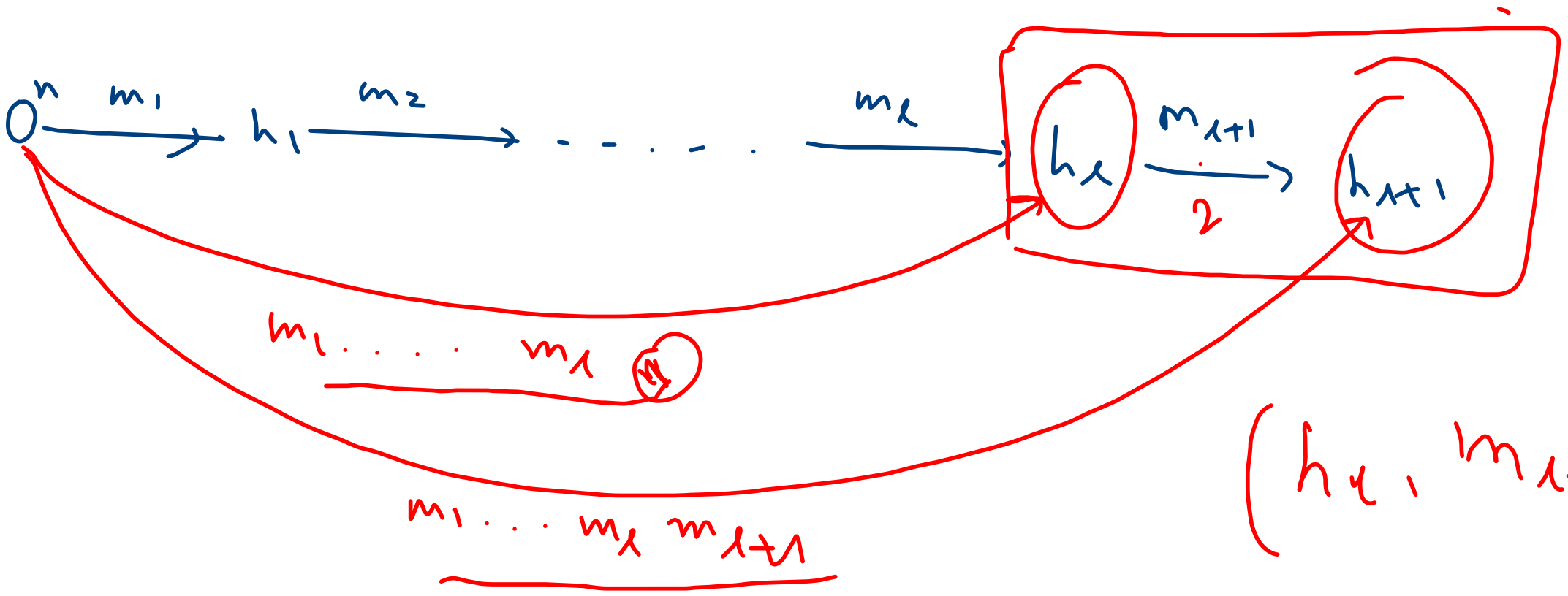
(*)



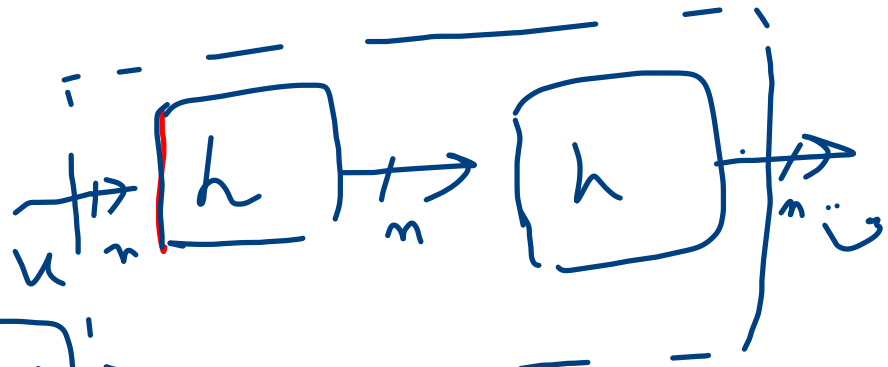

m
f
h
h'


m
h
h'


Big
Small
1. m1 .. mk
2. m1 .. mk+1
A
h1, mk+1

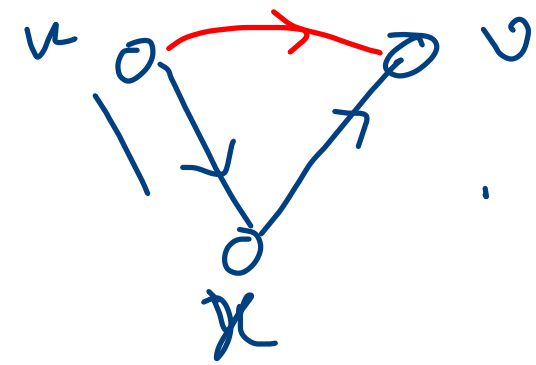

0
m1
h1
m2
mk
hk
mk+1
2
hk+1
m1 . . . . mk
m1 . . . mk mk+1

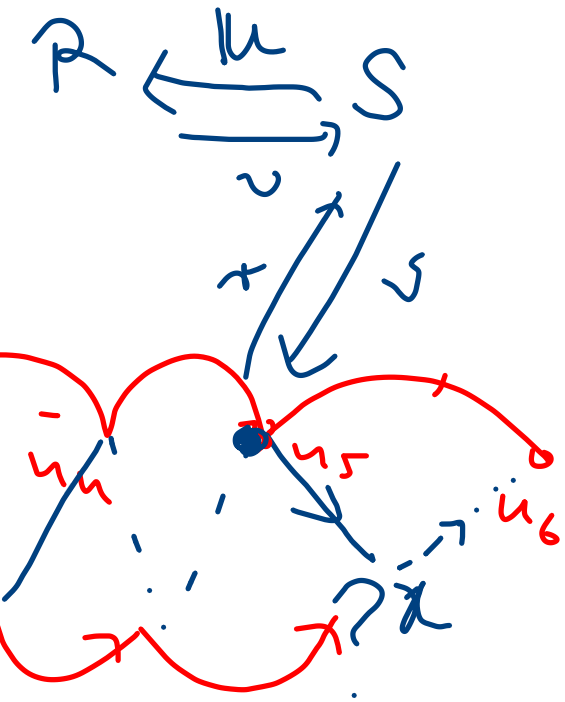
(h_k, m_{k+1})

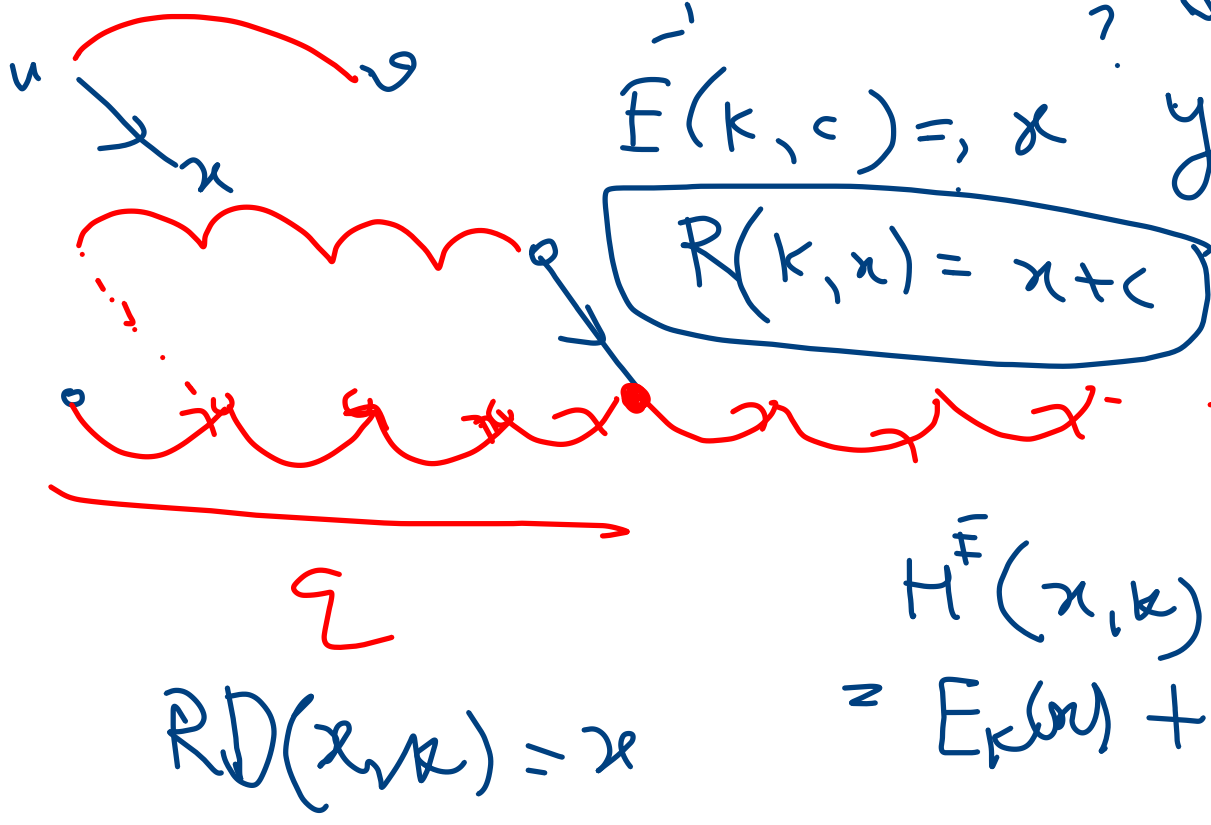


$h(u) = x$
$h(x) = v$

$h^2(u) = v$





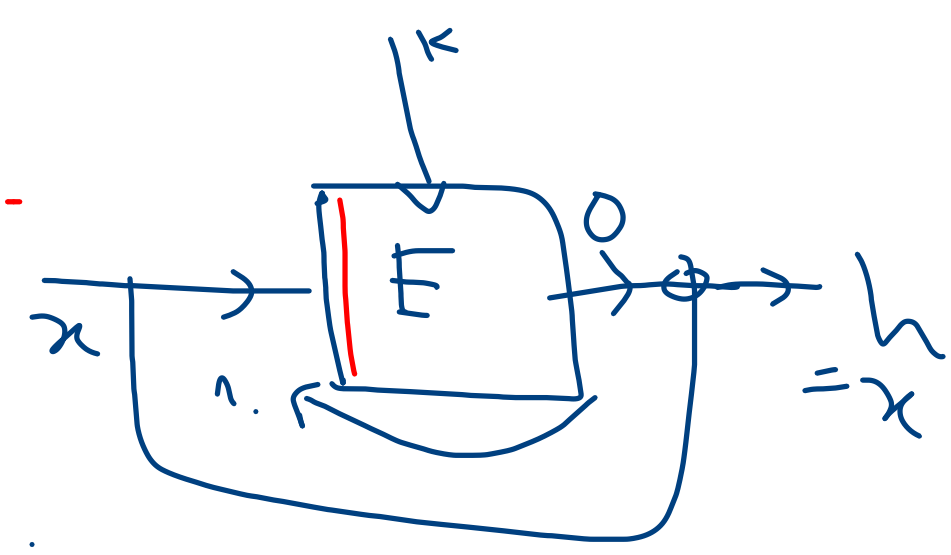


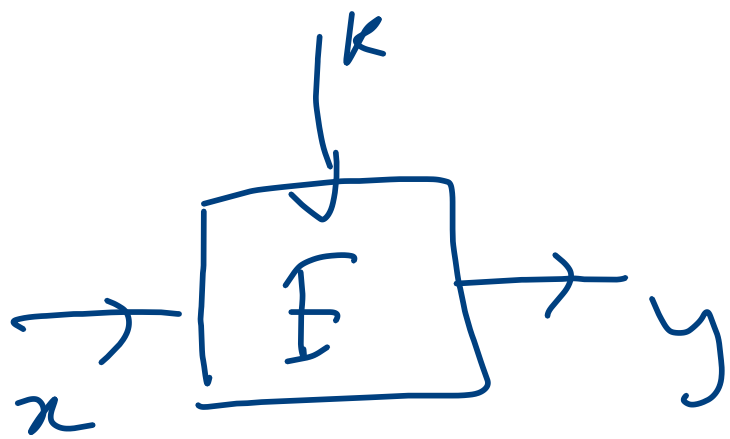
$E(k, c) = x$

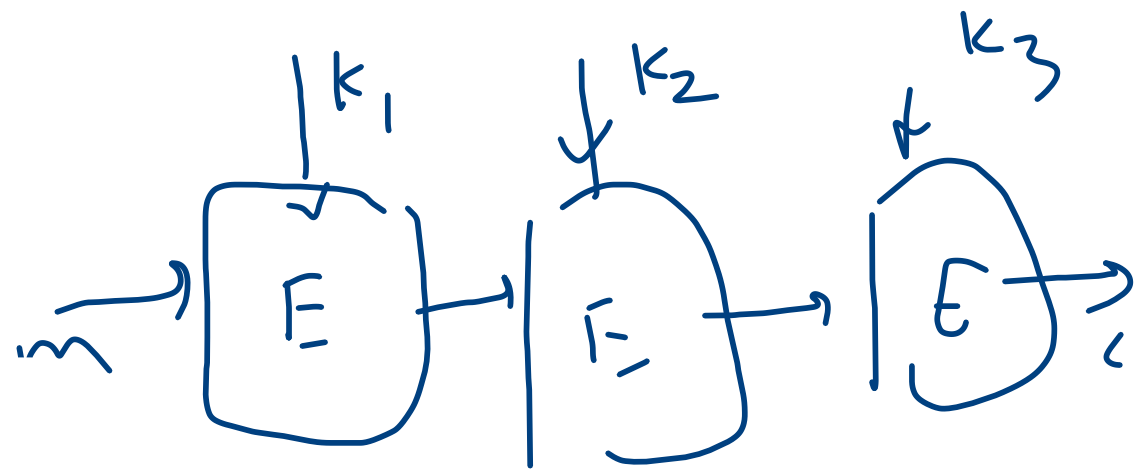
$R(k, x) = x + c$

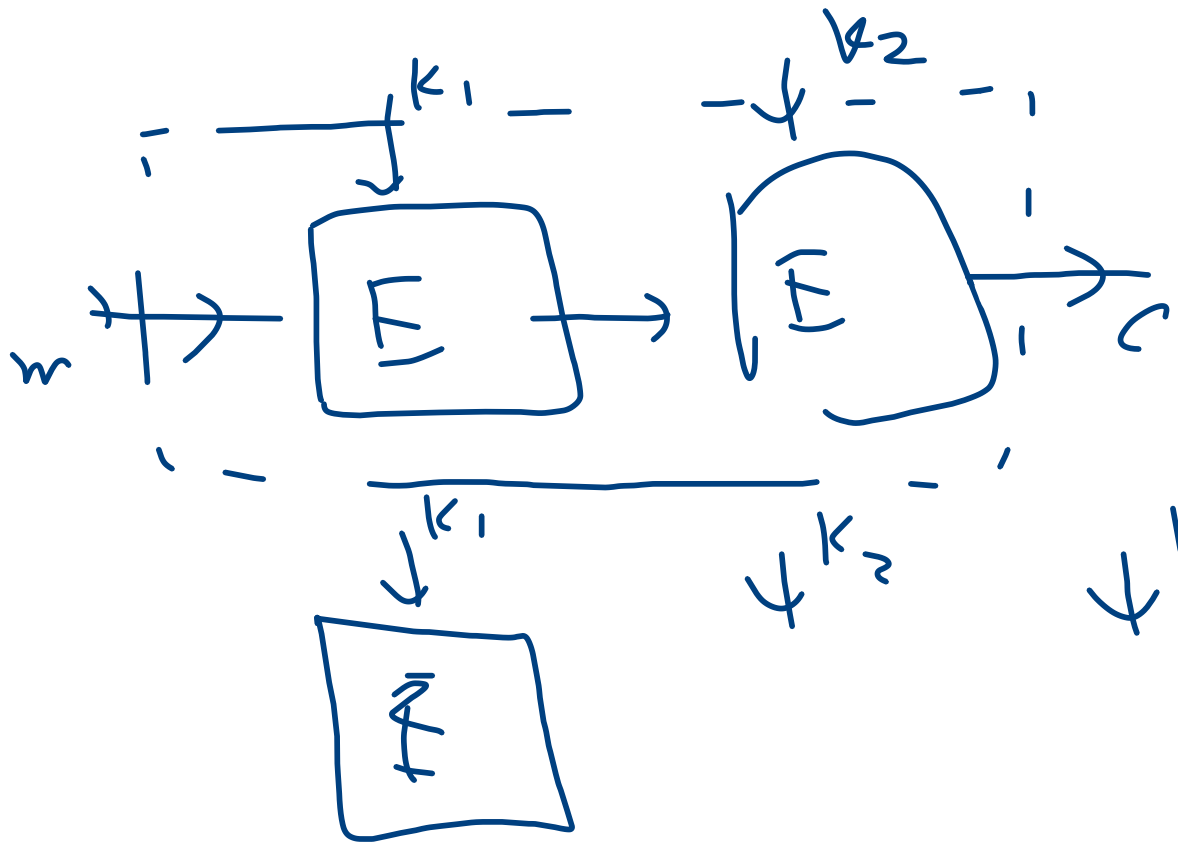
$RD(x, k) = x$

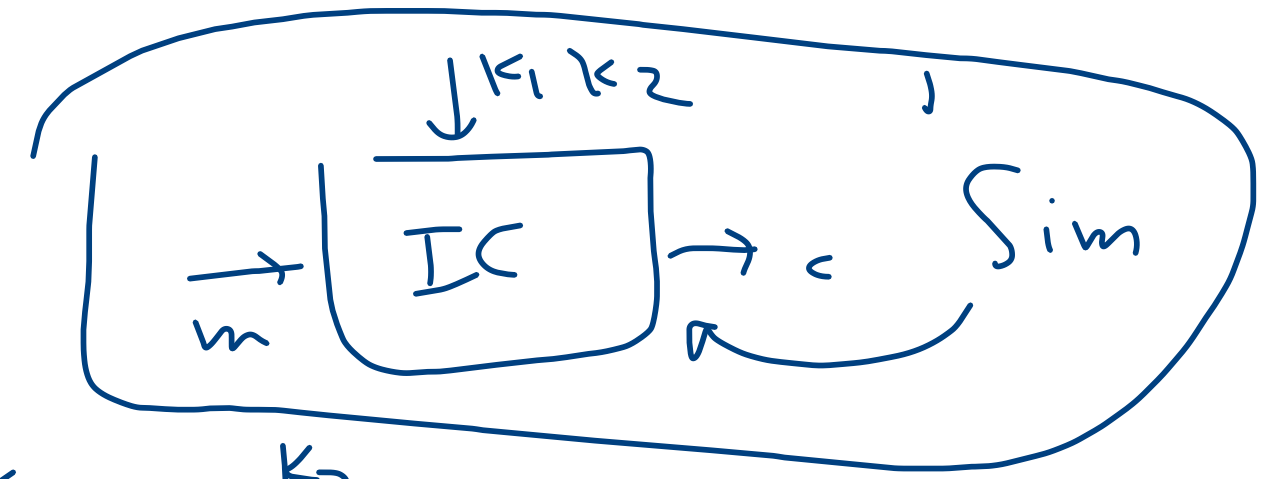
$H^E(x, k) = E_k(x) + x$




k
F
x
y


k1
k2
k3
F
F
F
m
c


k1
k2
F
F
m
c
k1
k2
f


k1 k2
IC
m
c
Sim
k1
k2