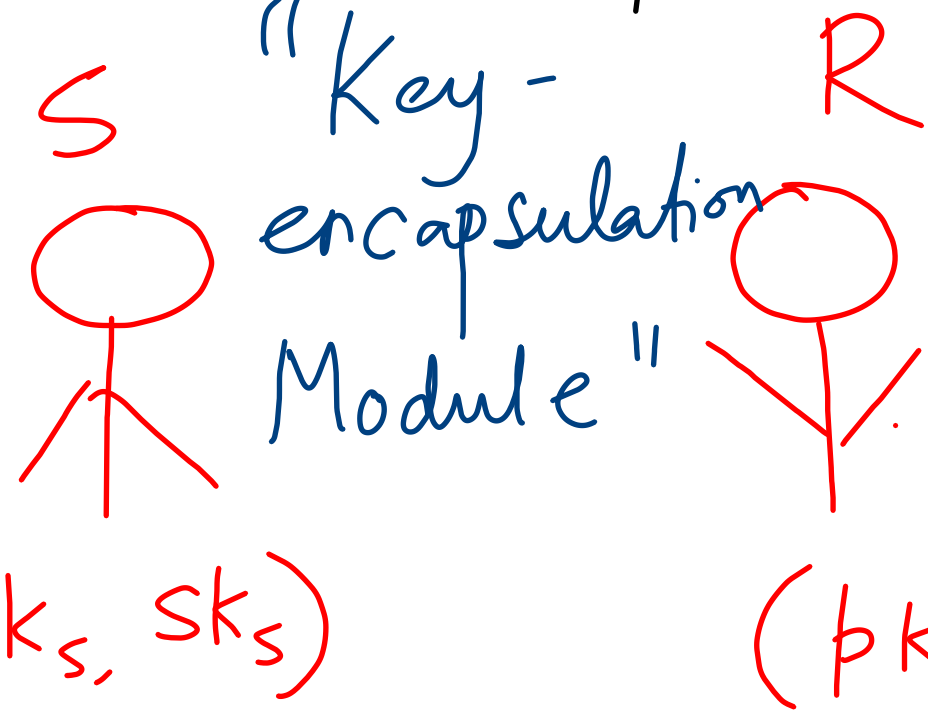
Hybrid Encryption:



Algorithm Π^{hy}.

On i/p n

- $(pk, sk) \leftarrow KGEN(1^n)$.
- $k \leftarrow\$ K$.
- To encrypt a message m computes $\left(c_1 \leftarrow Enc_{pk_R}(k),\ c_2 \leftarrow \mathcal{E}_k(m)\right)$.

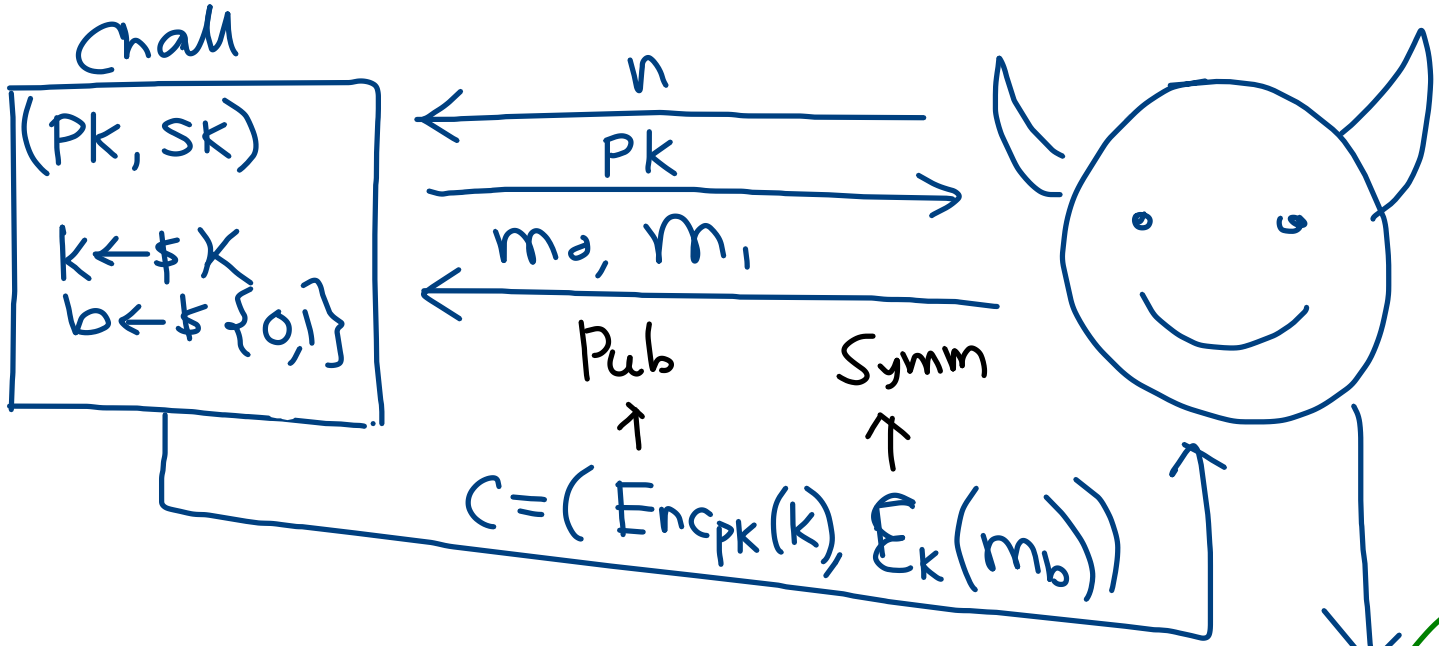
Send it to the receiver.

Enc is the public key enc. alg.
$\mathcal{E}$ is the symmetric " " mode.

Thm: If Π is a CPA-secure PKE scheme and Π' is a symmetric key encryption scheme that has indistinguishable encryptions in the presence of an eavesdropper, then Π^{hy} is a CPA-secure public key-encryption scheme.

Π is a PKE that can encrypts only 80 bit of message.
Suppose you want to encrypt a message of length 1680 bits.

Pf: To prove the theorem, it is enough to show that Π^{hy} is indistinguishable enc. in the presence of an eavesdropper.



Adversary wins if $b = b'$.

If the winning probability of this game for any adv. is small, then

$(pk, Enc_{pk}(k), E_k(m_0)) \approx_c (pk, Enc_{pk}(k), E_k(m_1))$

for a randomly chosen k.

Computationally indistinguishable.

μ, ν be two distr.

$\mu \approx_\varepsilon \nu$

$$\Delta = \left| P_{X \leftarrow \mu}[X = x] - P_{X \leftarrow \nu}[X = x] \right|$$

μ' be another distr.

$$\Delta \leq \left| P_{X \leftarrow \mu}[X = x] - P_{X \leftarrow \mu'}[X = x] \right| + \left| P_{X \leftarrow \mu}[X = x] - P_{X \leftarrow \nu'}[X = x] \right|$$
$$+ \left| P_{X \leftarrow \nu'}[X = x] - P_{X \leftarrow \nu}[X = x] \right|$$

(ν' " " " μ')

$D_1 = (pk, Enc_{pk}(k), \mathcal{E}_k(m_0)) \approx_c (pk, Enc_{pk}(k), \mathcal{E}_k(m_1))$ $= D_4$

claim 1 $\approx_c$ claim 3 $\approx_c$

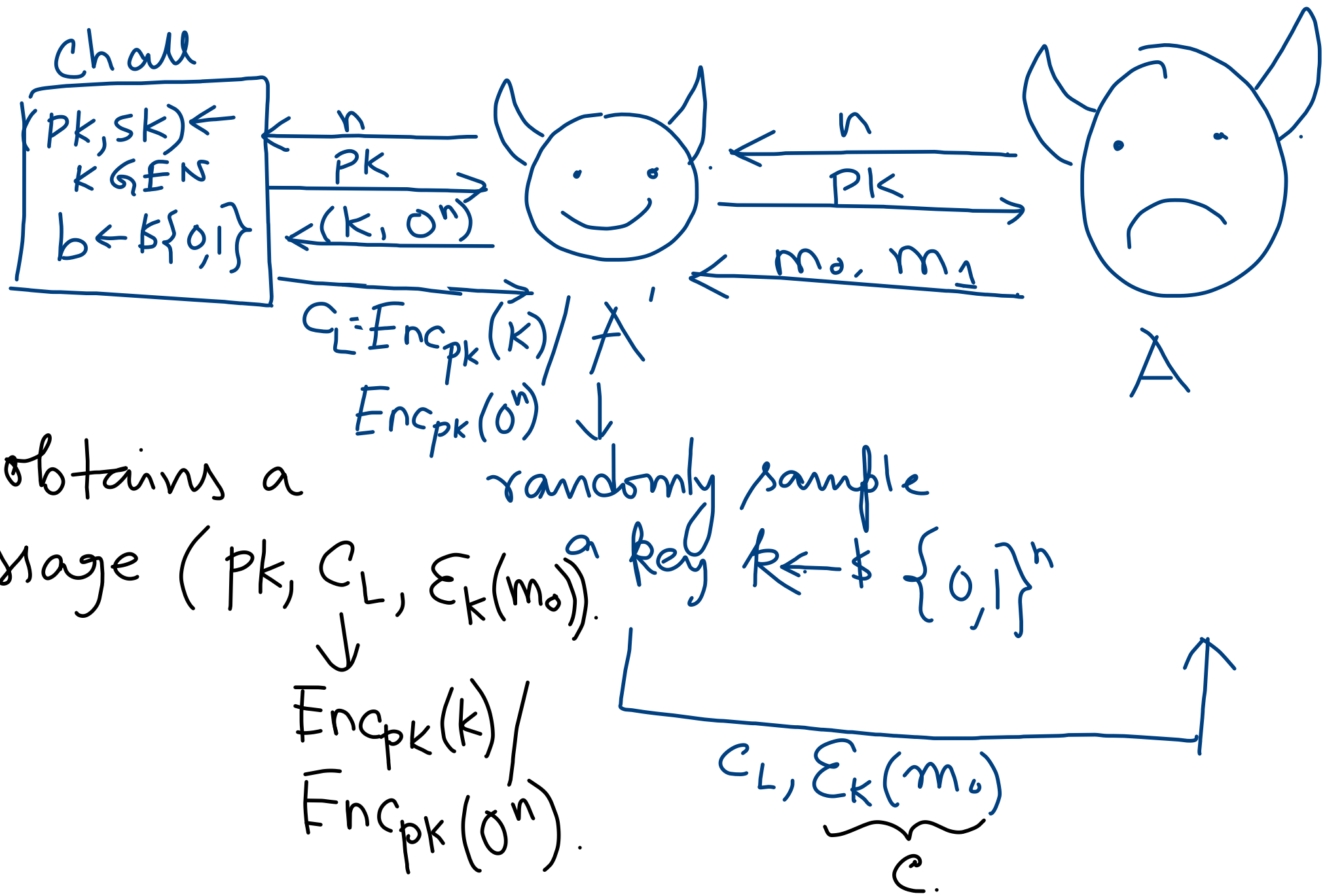
$D_2 = (pk, Enc_{pk}(0^n), \mathcal{E}_k(m_0)) \approx_c (pk, Enc_{pk}(0^n), \mathcal{E}_k(m_1))$ $= D_3$

claim 2

Claim 1:

If $\exists$ a PPT adv. A that distinguishes D_1 and D_4 then we show that $\exists$ a distinguisher A' that distinguishes the public key encryption Π in the presence of an eavesdropper.

We design a distingnisher A' as follows:



A' obtains a message $(pk, c_L, E_k(m_b))$.

A' runs A on i/p (c_L, c) and returns the bit b' if A outputs b'.

If $b=0$, A runs on an i/p which is distributed according to D_1.

If $b=1$, A runs on an i/p which is distributed according to D_2.

$$\Pr[A' \text{ outputs } 0 \mid b=0] = \Pr[A(y)=0]$$

$$\Pr[A' \text{ outputs } 1 \mid b=1] = \Pr_{\substack{y \leftarrow D_1 \\ y \leftarrow D_2}}[A(y)=1].$$

$$P_2\left[\mathrm{PubK}^{eav}_{A',\pi}(n)=1\right]$$

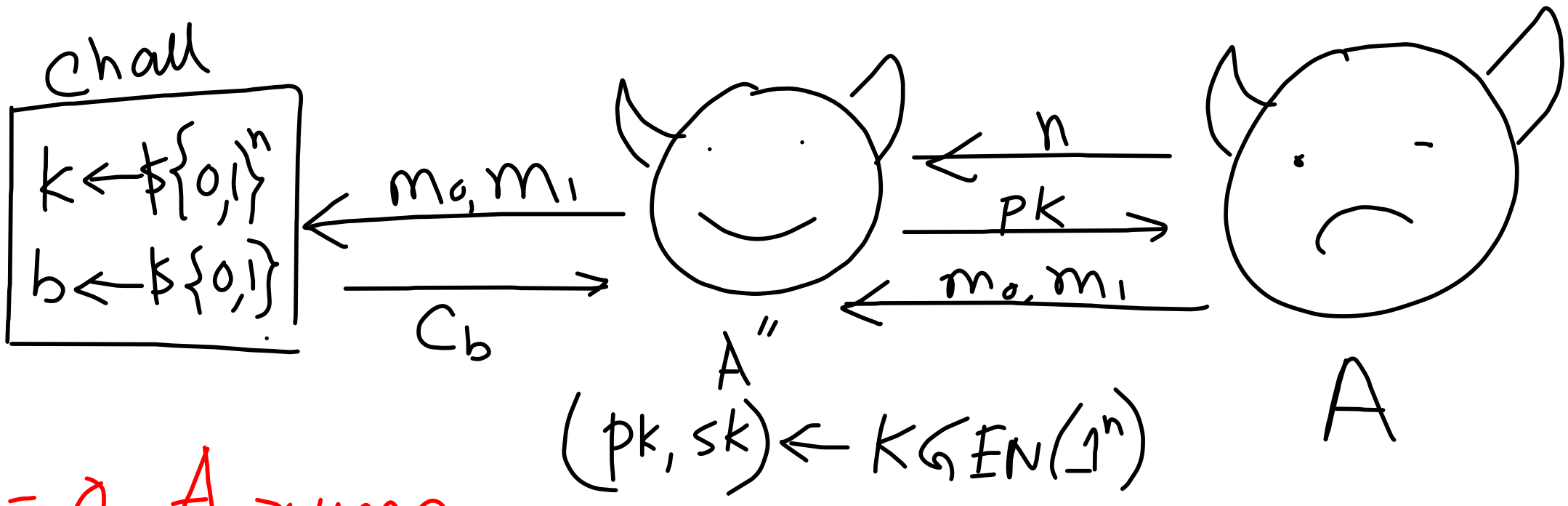
$$=\frac{1}{2}\,P_2[A' \text{ outputs } 0 \mid b=0]=\frac{1}{2}\cdot P_{y\leftarrow D_1}[A(y)=0]$$

$$+\frac{1}{2}\cdot P_2[A' \text{ outputs } 1 \mid b=1]=\frac{1}{2}\,P_{y\leftarrow D_2}[A(y)=1]$$

$$P\left[\mathrm{PubK}^{eav}_{A,\pi}(n)=1\right]=\frac{1}{2}\left\{\left[P_{y\leftarrow D_1}[A(y)=0]+P_{y\leftarrow D_2}[A(y)=1]\right]\right\}$$

$$\geq \frac{1}{2}+\varepsilon(n).$$

Claim 2:



If $b=0$, A runs on an i/p which is distributed according to D_2

If $b=1$, A runs on an i/p which is distributed according to D_3.

$$\Pr\left[\mathrm{Priv}K^{eav}_{A'',\pi'}(n)=1\right]$$

$$=\frac{1}{2}\cdot \Pr\left[A'' \text{ outputs } 0 \mid b=0\right] = \frac{1}{2}\cdot \Pr_{y\leftarrow D_2}\left[A(y)=0\right]$$

$$+\frac{1}{2}\cdot \Pr\left[A'' \text{ outputs } 1 \mid b=1\right] = \frac{1}{2}\cdot \Pr_{y\leftarrow D_3}\left[A(y)=1\right]$$

Therefore, we can see that,

$$\frac{1}{2}\left[\Pr_{y\leftarrow D_1}\left[A(y)=0\right] + \Pr_{y\leftarrow D_2}\left[A(y)=1\right]\right] \le \frac{1}{2}+\mathrm{negl}_1(n) \quad \text{— ①}$$

$$\frac{1}{2}\left[\Pr_{y\leftarrow D_2}\left[A(y)=0\right] + \Pr_{y\leftarrow D_3}\left[A(y)=1\right]\right] \le \frac{1}{2}+\mathrm{negl}_2(n) \quad \text{— ②}$$

$$\frac{1}{2}\left[\underset{y\leftarrow D_3}{P}[A(y)=0] + \underset{y\leftarrow D_4}{P}[A(y)=1]\right] \leq \frac{1}{2} + \text{negl}_3(n) \quad -③$$

From ①, ②, ③ we have to show,

$$\frac{1}{2}\left[\underset{y\leftarrow D_1}{P}[A(y)=0] + \underset{y\leftarrow D_4}{P}[A(y)=1]\right] \leq \frac{1}{2} + \text{negl}(n)$$

① + ② + ③

$$\frac{1}{2}\left[2 + \underset{y\leftarrow D_1}{P}[A(y)=0] + \underset{y\leftarrow D_4}{P}[A(y)=1]\right] \leq \frac{3}{2} + \text{negl}(n)$$

$$\Rightarrow \frac{1}{2}\left[\underset{y\leftarrow D_1}{P}[A(y)=0] + \underset{y\leftarrow D_4}{P}[A(y)=1]\right] \leq \frac{1}{2} + \text{negl}(n).$$