Pseudorandom Functions

A family of functions $\mathcal{F}: \left\{ F_k : \{0,1\}^n \to \{0,1\}^\ell \right\}_{k \in \{0,1\}^\lambda}$

We want:

1) Efficiency: $\forall k \in \{0,1\}^\lambda$
   $\forall x \in \{0,1\}^n$
   then $F_k(x)$ is computable in poly-time

2) Pseudorandom:
   It looks like a $\underbrace{\text{random}}$ function $\forall$ PPT $\mathcal{A}$

   → means that its truth table is randomly chosen

$\text{REAL}_{\mathcal{F},\mathcal{A}}(\lambda)$

$\mathcal{A}(1^\lambda)$ $\qquad\qquad$ $\mathcal{C}(1^\lambda)$

poly(λ)

$\xrightarrow{x \in \{0,1\}^\lambda}$ $\quad k \leftarrow \$ \{0,1\}^\lambda$

$\longleftarrow$ $\quad y = F_k(x)$

$\xrightarrow{b'}$

b' → if $\mathcal{A}$ thinks $\mathcal{C}$ is from REAL or from RAND

$\text{RAND}_{\mathcal{R},\mathcal{A}}(\lambda)$ (we compare REAL with RAND)

$\mathcal{A}(1^\lambda)$ $\qquad\qquad$ $\mathcal{C}(1^\lambda)$

$\xrightarrow{x}$ $\quad R \leftarrow \$ \mathcal{R}(\lambda, n, \ell)$

$\xleftarrow{y = R(x)}$

↳ set of all functions mapping

$$\xrightarrow{\quad b' \quad}$$ $n(\lambda)$ bits into $\ell(\lambda)$ bits

DEF Family $\mathcal{F}$ IS PSEUDORANDOM IF

$$\forall \text{PPT } A : \left\{ \text{REAL}_{\mathcal{F},A}(\lambda) \right\}_\lambda \approx_c \left\{ \text{RAND}_{\mathcal{R},A}(\lambda) \right\}_\lambda$$

PLAN: 1) PRFs $\Rightarrow$ CPA SKE

2) How to construct PRFs?

Recall: we started with ONE-TIME PAD

$$Enc(k,m) = k \oplus m$$

then we used PRGs

$$Enc(k,m) = G(k) \oplus m$$ this allows for a short key but still one time SKE

Let $\mathcal{F}$ be a PRF-family. Define $\Pi(Enc, Dec)$ as

$$Enc(k,m) = (r, F_k(r) \oplus m)$$
$$= (c_1, c_2) \text{ for } r \leftarrow \$ \{0,1\}^n$$

$$Dec(k, c_1, c_2) = F_k(c_1) \oplus c_2$$

$$\mathcal{M} = \{0,1\}^\ell ; \mathcal{K} = \{0,1\}^\lambda$$

THM: If F is a PRF, then above Π is CPA secure.

PROOF: Start with CPA experiment:

$$\text{GAME}^{CPA}_{\Pi,A}(\lambda,b) \equiv H_0(\lambda,b)$$

$$\begin{array}{lcl}
\mathcal{A}(1^\lambda) & & \mathcal{C}(1^\lambda) \quad k \leftarrow \$ \{0,1\}^\lambda \\
 & \xrightarrow{\qquad m_i \qquad} & \\
 & \xleftarrow{\qquad c_i \qquad} & c_i = (r_i, F_k(r_i) \oplus m_i) \\
 & & \quad r_i \leftarrow \$ \{0,1\}^n \\
 & \xrightarrow{\qquad m_0^*, m_1^* \qquad} & c^* = (r^*, F_k(r^*) \oplus m_b^*) \\
 & \xleftarrow{\qquad c^* \qquad} & \quad r^* \leftarrow \$ \{0,1\}^n \\
 & \xrightarrow{\qquad m_i \qquad} & \\
 & \xleftarrow{\qquad c_i \qquad} & \\
 & \xrightarrow{\qquad b' \qquad} &
\end{array}$$

We need: $\forall$ PPT $\mathcal{A}$: $H_0(\lambda,0) \approx_c H_0(\lambda,1)$

We define $H_1(\lambda,b)$ (↗ an idealized experiment), in which instead of picking a random k, we pick a random truth table $R \leftarrow \$ \mathcal{R}(\lambda,n,\ell)$.

In this way, $c_i = (r_i, R(r_i) \oplus m_i)$, $r_i \leftarrow \$ \{0,1\}^n$

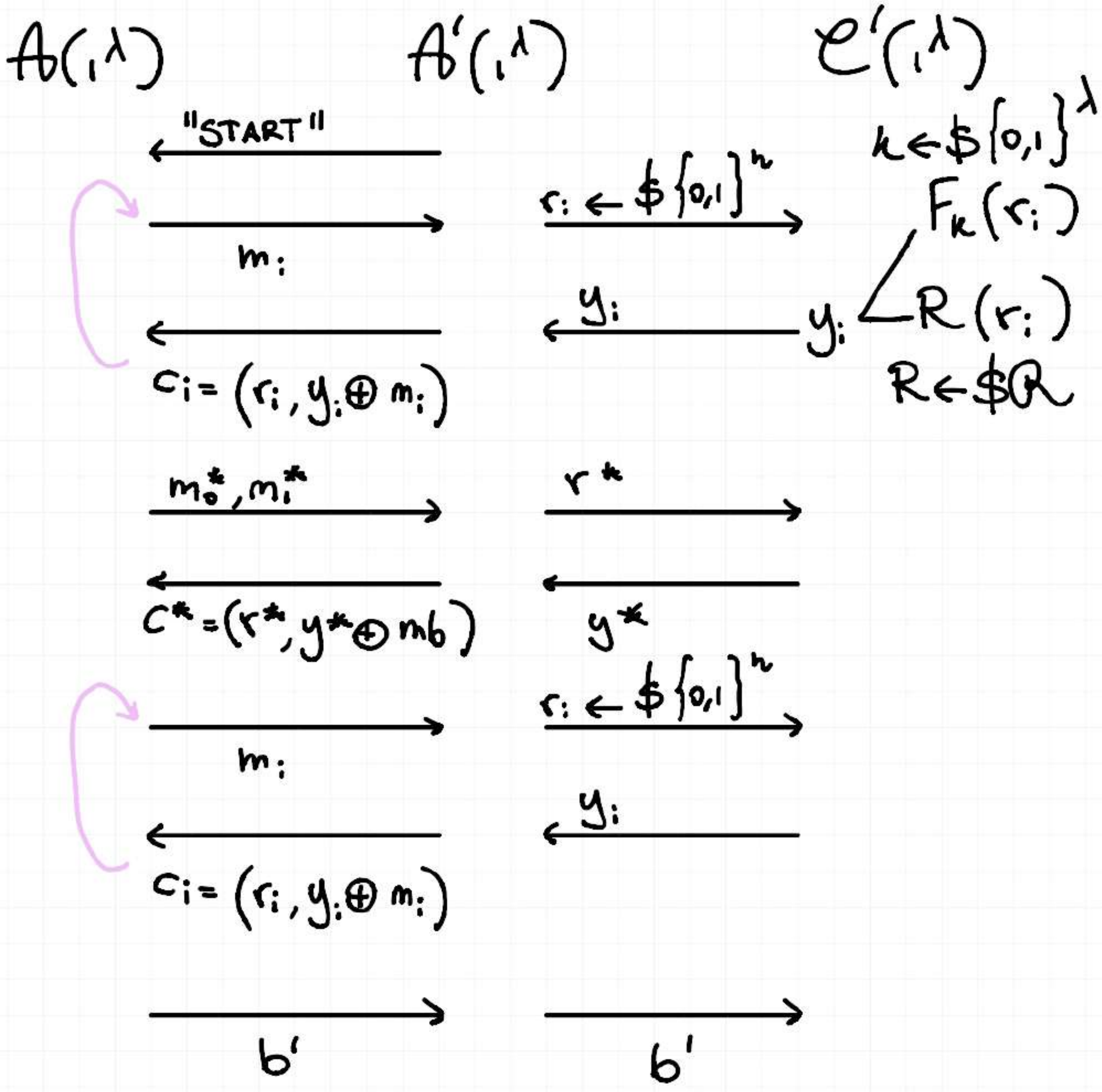
$$c^* = (r^*, R(r^*) \oplus m_b^*), \; r^* \leftarrow \$ \{0,1\}^n$$

LEMMA: $\forall b \in \{0,1\}: \{H_0(\lambda, b)\} \approx_c \{H_1(\lambda, b)\}$

PROOF: Fix b. Assume $\nexists$ PPT $\mathcal{A}$ such that

$$\left| \Pr[H_0(\lambda,b)=1] - \Pr[H_1(\lambda,b)=1] \right| \geq 1/poly(\lambda)$$

We define a reduction $\mathcal{A}'$ attacking $\mathcal{F}$



Analysis: Perfect simulation (excercise)

Let's also introduce $H_2(\lambda, b)$, which is impossible to break for A (it's still a mental experiment, though).

In H_2, we don't pick any key, but we just extract random c.

$c_i = (u_i, v_i)$

$$\begin{matrix} u_1 \leftarrow \$ \{0,1\}^n \\ u_2 \leftarrow \$ \{0,1\}^\ell \end{matrix} \Rightarrow \begin{matrix} c^* = (u^*, v^*) \\ u^* \leftarrow \$ \{0,1\}^n \\ v^* \leftarrow \$ \{0,1\}^\ell \end{matrix}$$

We want to prove that A can't distinguish H_1 from H_2

<u>LEMMA</u>: $\forall A$ (even UNBOUNDED), $\forall b \in \{0,1\}$

$$SD(H_1(\lambda, b), H_2(\lambda, b)) \leq negl(\lambda)$$

or

$$|Pr[H_1(\lambda, b) = 1] - Pr[H_2(\lambda, b) = 1]| \leq negl(\lambda)$$

Let E be the event that $(r_1 \dots r_q, r^*)$ (not distinct) for $q = poly(\lambda)$.

Then, if $\overline{E}$ happens then $H_1(\lambda, b) \equiv H_2(\lambda, b)$

<u>CLAIM</u>: $\forall A, \forall b$, for any event E

$$|Pr[H_1(\lambda, b) = 1] - Pr[H_2(\lambda, b) = 1]| \leq Pr[E]$$

$$Pr[E] = Pr[\exists i, j \in [q] ; r_i = r_j] \quad (i \neq j)$$

$$\leq \sum_{i,j} Pr[r_i = r_j] \quad \text{UNION BOUND}$$

$$= \sum_i Col(U_n) \leq 2^{-n} \cdot \binom{q}{2}$$

$$= negl(\lambda) \cdot poly(\lambda) = negl(\lambda)$$

And of course: $H_2(\lambda, 0) \equiv H_2(\lambda, 1)$

Proof of technical claim:

$$|Pr[H_1(\lambda,b)=1] - Pr[H_2(\lambda,b)=1]|$$

$$= |Pr[H_1(\lambda,b)=1 \wedge E] + Pr[H_1(\lambda,b)=1 \wedge \bar{E}]$$
$$- Pr[H_2(\lambda,b)=1 \wedge E] + Pr[H_2(\lambda,b)=1 \wedge \bar{E}]|$$

$$= |Pr[E] \cdot Pr[H_1(\lambda,b)=1 | E] -$$
$$Pr[E] \cdot Pr[H_2(\lambda,b)=1 | E]| +$$
$$Pr[\bar{E}] \cdot Pr[H_1(\lambda,b)=1 | \bar{E}] -$$
$$Pr[\bar{E}] \cdot Pr[H_2(\lambda,b)=1 | \bar{E}]|$$

when the event doesn't happen $\rightsquigarrow$ it's ϕ

$$\leq Pr[E] \cdot |\text{ stuff } | E| + Pr[\bar{E}] \cdot \phi$$