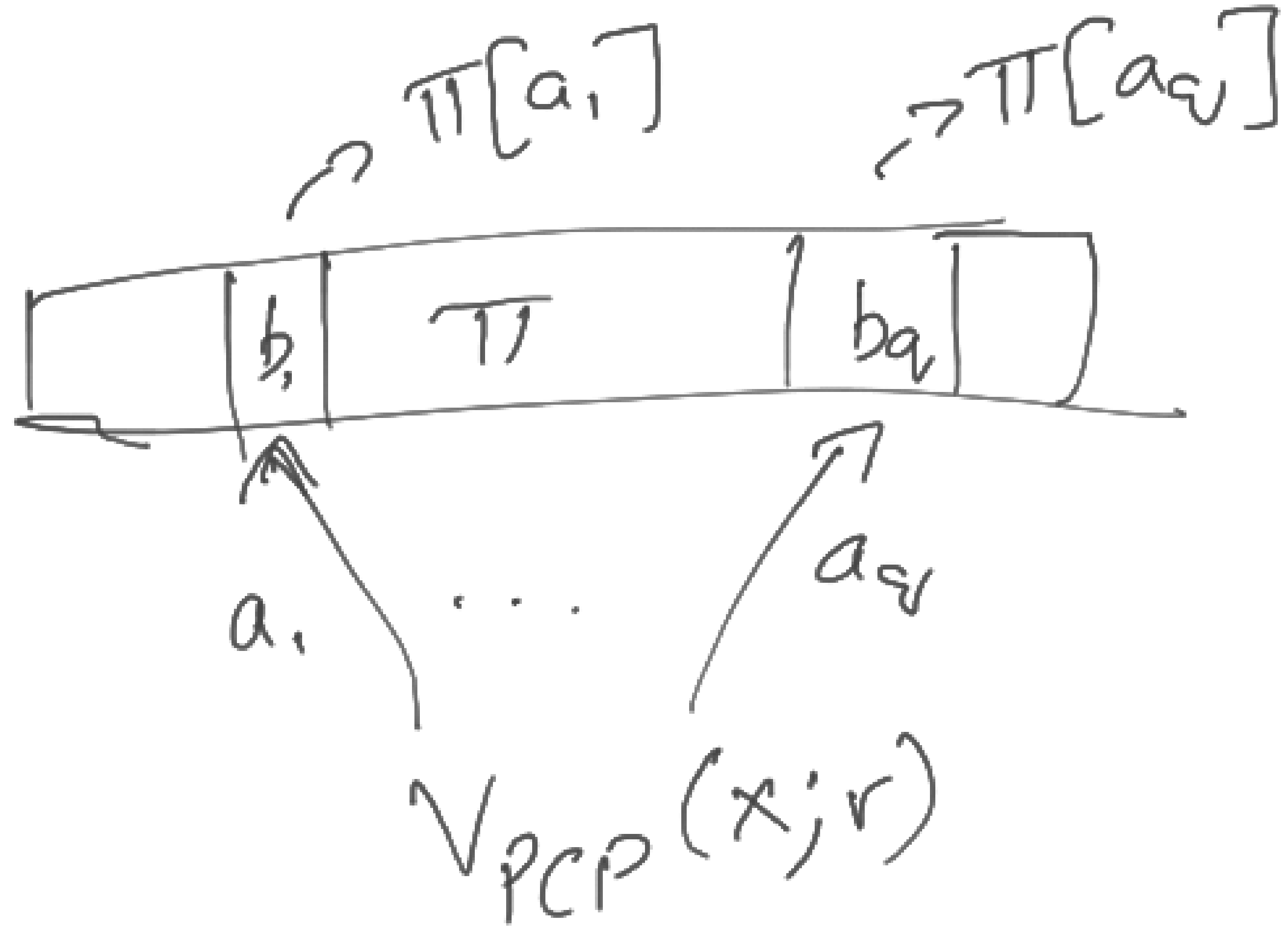
Arguments from PCPs



$V(x, b_1, \ldots, b_q; r)$

$\downarrow$

acc/rej

$P(w) \quad \times \quad V$

$w \to \pi$

$a_1, \ldots, a_q \leftarrow V_{PCP}(x;r)$

$\xrightarrow{\text{Commit}(\pi)}$

$\xleftarrow{a_1, \ldots, a_q}$

$b_i \leftarrow \pi[a_i]$ "Decommit"

$\xrightarrow{\pi[a_1], \ldots, \pi[a_q]}$

$V_{PCP}(x, b_1, \ldots, b_q; r)$

$\to$ acc/rej

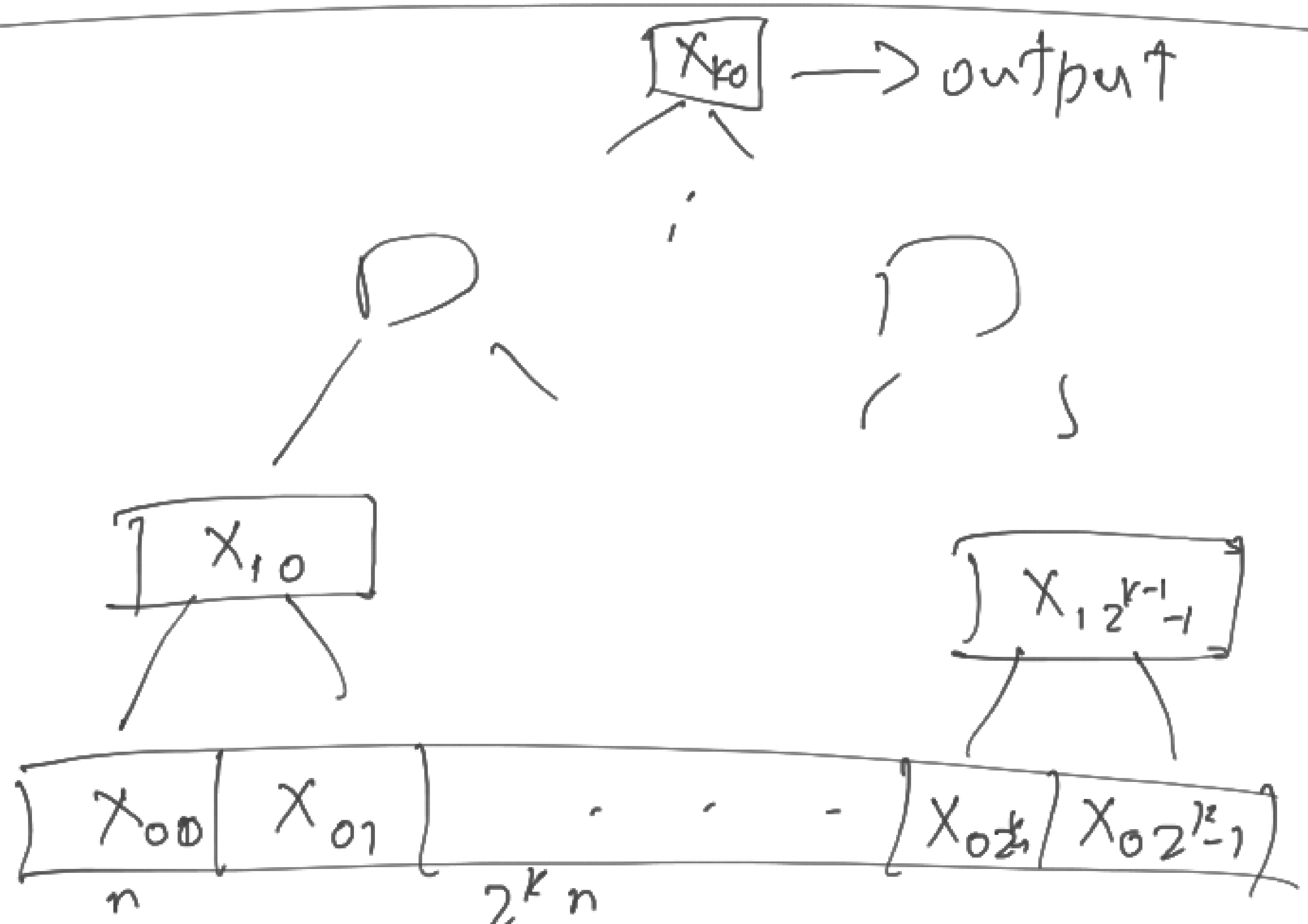
CRHF: $H = \{ h : \{0,1\}^{2n} \to \{0,1\}^n \}$

$$\forall \text{PPT } A: \Pr_{\substack{h \leftarrow H \\ (x,x') \leftarrow A(h)}} [x \neq x' \wedge h(x) = h(x')] < \text{negl}(n)$$

Merkle Hashing:

$h^k : \{0,1\}^{2^k n} \to \{0,1\}^n$

$x_{ij} = h(x_{i+1,2j}, x_{i+1,2j+1})$



$S(x)$ $\qquad\qquad$ R

$x \in \{0,1\}^{2^k n}$ $\qquad\qquad$ $h \leftarrow H$

$\xleftarrow{\ h\ }$

$y \leftarrow h^k(x)$

$\xrightarrow{\ y\ }$

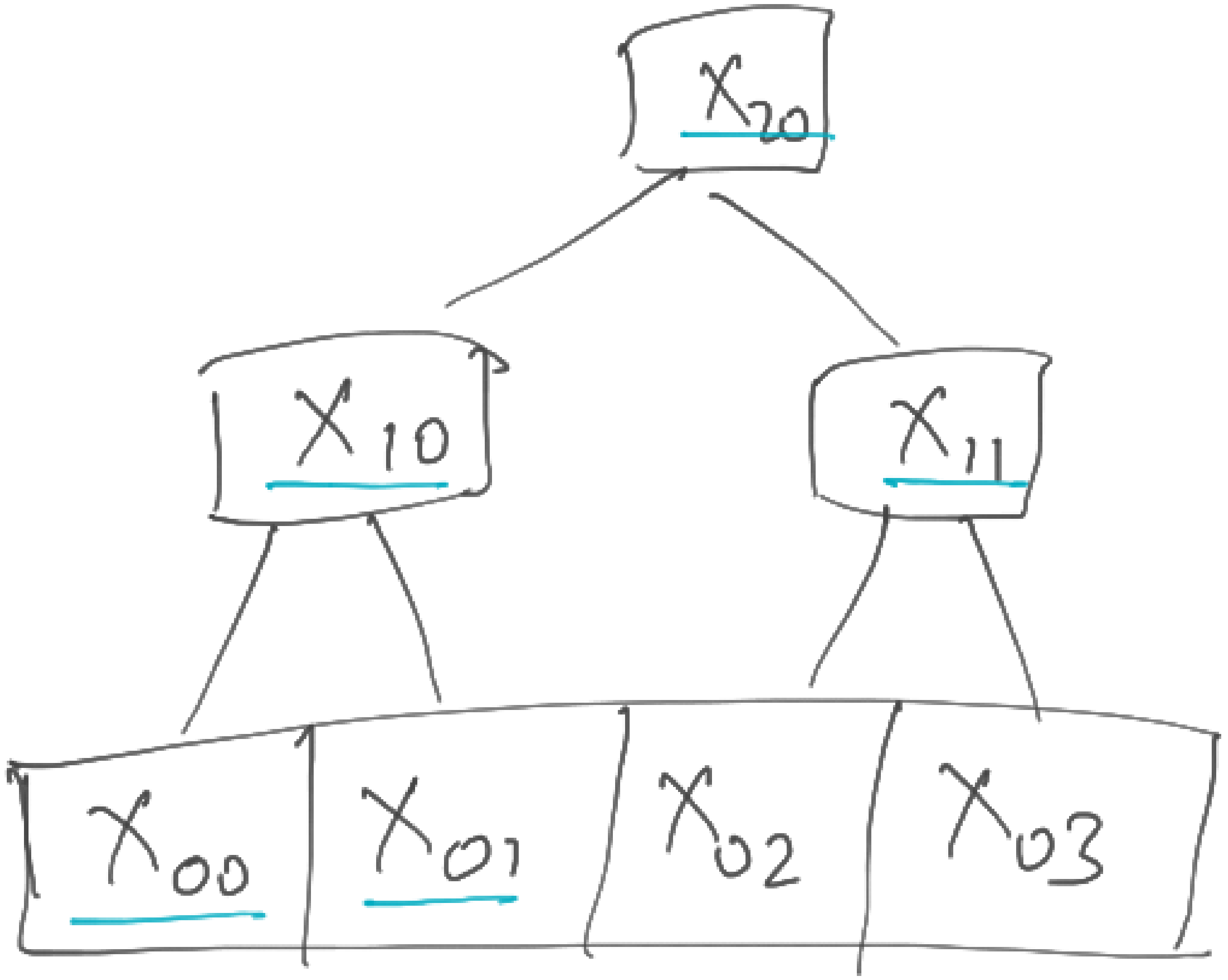
commit

$\xleftarrow{\ i\ }$

Decommit

send x_{0i} and all labels on path to root with siblings $\longrightarrow$

Check all hashes along path



$S(x)$ $\qquad\qquad$ R

$\xleftarrow{\ i=0\ }$

$\xrightarrow{\ x_{00},\, x_{01}\ }$

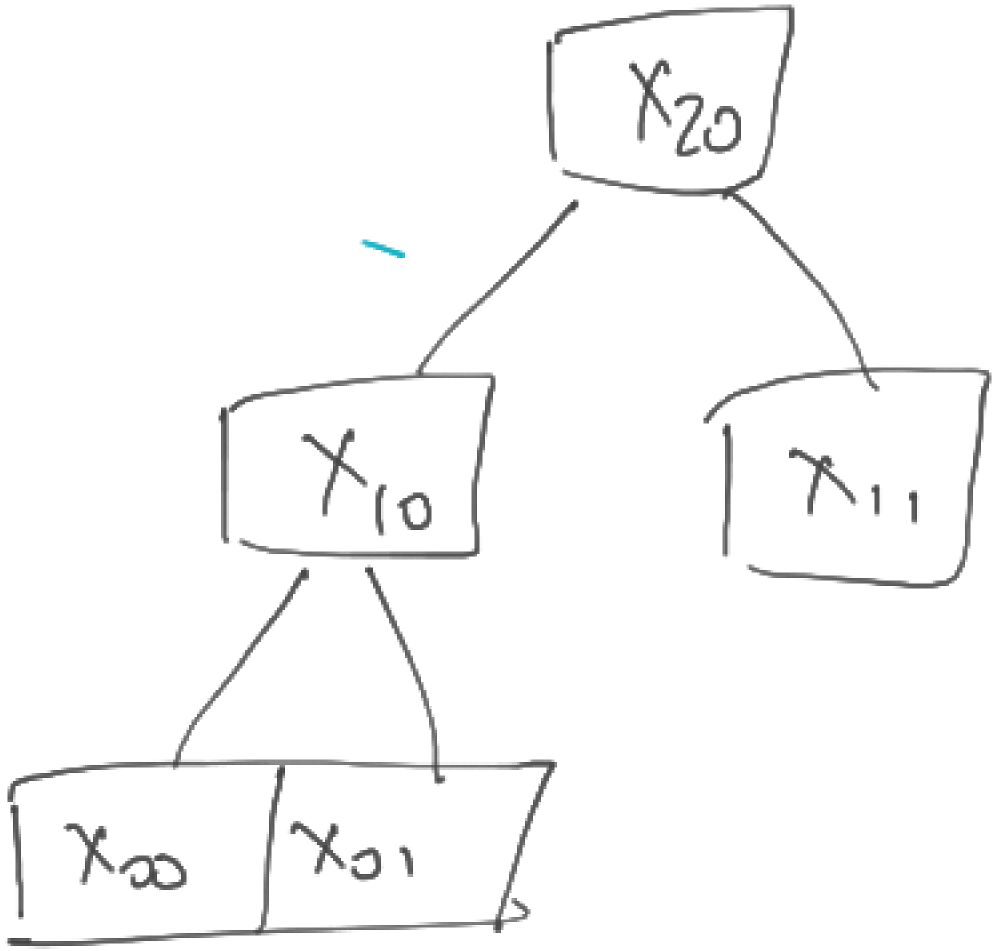
$x_{10},\, x_{11}$

x_{20}

$x_{10} = h(x_{00}, x_{01})$

$x_{20} = h(x_{10}, x_{11})$

$y = x_{20}$



$x_{10} = x_{10}'$

$x_{10} \neq x_{10}'$

Commitment: y

Sender sent: $x_{00}, x_{01}, x_{10}, x_{11}, x_{20}$

$x_{00}', x_{01}', x_{10}', x_{11}', x_{20}'$

$x_{20} = y$ $\qquad$ $x_{20}' = y$

$x_{20} = h(x_{10}, x_{11})$ $\qquad$ $x_{20}' = h(x_{10}', x_{11}')$

$x_{10} = h(\underline{x_{00}, x_{01}})$ $\qquad$ $x_{10}' = h(\underline{x_{00}', x_{01}'})$

$P(w)$ $\qquad x \qquad$ V

$w \to \pi$ $\qquad\qquad$ $h \leftarrow H$

$\xleftarrow{\quad h \quad}$

$y \leftarrow h^k(\pi)$

$\xrightarrow{\quad y \quad}$

$\xleftarrow{\quad a_1, \ldots, a_q \quad}$

$\longrightarrow$ $\qquad$ $V_{PCP}(\ldots)$

Decommit corresponding blocks of π $\qquad$ $\downarrow$

acc/rej

<u>Claim:</u> for any efficient det. P^*:

$$\Pr_{h \leftarrow H}[P^* \text{ is not consistent}] < \text{negl}(n)$$

P^* consistent $\Rightarrow$ can recover PCP oracle π^*

For $x \notin L$:

$$\Pr[V \text{ accepts}] \leq \Pr[P^* \text{ not consistent}] + \Pr[V_{PCP} \text{ acc} \mid P^* \text{ is consistent}]$$

P^* consistent $\Rightarrow$ $\exists \Pi^*$ s.t. in response to $(a_1, \dots, a_q)$,
P^* "sends" $(\Pi^*[a_1], \dots, \Pi^*[a_q])$

P^* non-consistent $\Rightarrow$ $\exists\, a$ and two sets of queries
$(a_1, \dots, a_q)$ and $(a_1', \dots, a_q')$

$a_1 = a$, $a_q' = a$

$(b_1, \dots, b_q)$ $\quad$ $(b_1' \dots b_q')$

$b_1 \neq b_q'$

$\forall P^*$

$\exists A$ s.t. $\forall h$: P^* non-consistent given V sent h $\Rightarrow$ A finds collision for h

$A(h)$:

- Simulate (P^*, V) with V sending first message h.
- P^* (in simulation) responds with y
- For all possible random string r for V_{PCP}:
  - $(a_1, \ldots, a_q) \leftarrow V_{PCP}(x; r)$
  - Get $(b_1, \ldots, b_q) \leftarrow P^*(a_1 \ldots a_q)$, record them if it passes
- Find query a that is answered inconsistently

Fiat-Shamir Transformation

$$
\begin{array}{ccc}
P & x & V \\
 & \xrightarrow{\quad \alpha \quad} & \\
 & \xleftarrow{\quad \beta \quad} & \\
 & \xrightarrow{\quad \gamma \quad} & V(x,\alpha,\beta,\gamma) \\
 & & \downarrow \\
 & & \text{acc/rej}
\end{array}
\quad \longrightarrow \quad
\begin{array}{ccc}
P & x & V \\
 & \xrightarrow{\quad \pi \quad} & \\
 & & V(x,\pi) \\
 & & \downarrow \\
 & & \text{acc/rej}
\end{array}
$$

$\alpha \in \{0,1\}^a$, $\gamma \in \{0,1\}^c$, $\beta \leftarrow \{0,1\}^b$

$$P_{FS} \qquad\qquad x \qquad\qquad V_{FS}$$

$\alpha \leftarrow P(x)$

$\beta \leftarrow H(x,\alpha)$

$r \leftarrow P(x,\alpha,\beta)$

$$\xrightarrow{(\alpha,\beta,r)}$$

Check $\beta = H(x,\alpha)$

$V(x,\alpha,\beta,r) \to$ acc/rej

Random Oracle Model:

$$O : \{0,1\}^m \longrightarrow \{0,1\}^\ell$$

A^O

$O(0^m), \ldots, O(1^m)$

uniform and independent

$P \quad x \quad V$

$\xrightarrow{\quad \alpha \quad}$

$\xleftarrow{\quad \beta \quad}$

$\xrightarrow{\quad \gamma \quad}$

$P_{FS}^{O} \quad x \quad V_{FS}^{O}$

$\alpha \leftarrow P(x)$

$\beta \leftarrow O(x,\alpha)$

$\gamma \leftarrow P(x,\alpha,\beta) \xrightarrow{(\alpha,\beta,\gamma)}$

$\beta = O(x,\alpha)$

$V(x,\alpha,\beta,\gamma)$

Public-coin argument
negl. soundness error
with $O(1)$ messages
$\longrightarrow$
Non-interactive argument
in Random Oracle Model

Fix $x \notin L$

- β is bad for α if $\exists r$ s.t. $V(x, \alpha, \beta, r)$ accepts

P^{*}'s objective: find α s.t. $O(x, \alpha)$ is bad for α

$\forall \alpha$: $\Pr\left[O(x, \alpha) \text{ is bad for } \alpha\right] <$ negl

<u>Correlation Intractable:</u> can't find α s.t. $O(x, \alpha)$ is bad for α

P_{fs}^*: α somehow

$\beta \leftarrow O(x, \alpha)$ output (α, β, γ)

γ somehow

Semi-honest prover

If $\exists$ semi-honest P_{fs}^* s.t. (P_{fs}^*, V_{fs}) accepts with non-negl. prob. $\Rightarrow \exists P^*$ s.t. (P^*, V) accepts with non-negl. prob.

P^* $\qquad$ x $\qquad$ V

Run P^*_{fs} until it makes query (x, α)

$\xrightarrow{\alpha}$

$\xleftarrow{\beta}$

Send β to P^*_{fs} as response.

Resume P^*_{fs} till it outputs (α, β, γ) $\xrightarrow{\gamma}$

$\Pr[(P^*, V) \text{ accepts}]$

$=$

$\Pr_{O}[(P^{*O}_{fs}, V^{O}_{fs}) \text{ accepts}]$

P^*_{fs} queried $O(x, \alpha)$ to get β, then computed γ

$V \quad (x, \alpha, \beta, \gamma)$

Same in (P^*, V)!

w.l.o.g: 1. If P^*_{fs} runs in time T, it makes at most T oracle queries

2. If P^*_{fs} outputs (α, β, γ), then it makes the query $O(x, \alpha)$ at some point (and the response to this was β)

P^* $\qquad$ x $\qquad$ V

- Sample $i \leftarrow [T]$
- Run P_{fs}^*, responding to queries uniformly randomly until i^{th} query (x, α) is made

$\xrightarrow{\alpha}$

$\xleftarrow{\beta}$

- Respond with β
- If P_{fs}^* outputs (α, β, r) $\xrightarrow{r}$
else abort

$$\Pr[(P^*, V) \text{ acc}] \geq \left[\frac{\Pr[(P_{fs}^*, V_{fs}^*) \text{ accepts}]}{T}\right]$$

P $\qquad\qquad$ V $\qquad\qquad\qquad$ P_{FS} $\qquad\qquad$ V_{FS}

$$\xrightarrow{\quad\alpha_1\quad}$$

$$\xleftarrow{\quad\beta_1\quad}$$

$$\xrightarrow{\quad\alpha_2\quad}$$

$$\xleftarrow{\quad\beta_2\quad}$$

$\vdots$

$$\alpha_1 \leftarrow P(x)$$

$$\beta_1 \leftarrow O(x, \alpha_1)$$

$$\alpha_2 \leftarrow P(x, \alpha_1, \beta_1)$$

$$\beta_2 \leftarrow O(x, \alpha_1, \alpha_2)$$

$\vdots$

$$\longrightarrow$$