Power of CZK

$NP \subseteq CZK$

$IP \subseteq CZK$

assuming commitments or PRFs

P × V

α_1

β_1

α_2

β_k

$V(\alpha_1, \ldots, \beta_k) \rightarrow$ accept

$L \in IP$ Public-coin protocol (P, V)

P' × V'

α_1

$comm(\beta_1)$

α_2

$comm(\beta_2)$

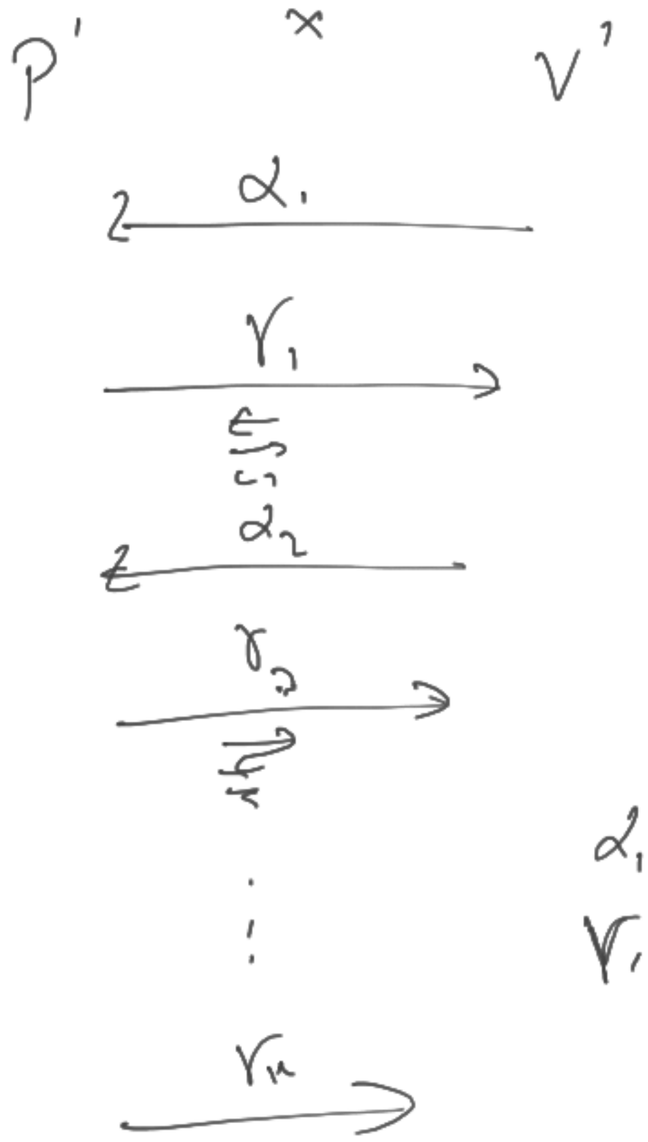
$comm(\beta_k)$

$\alpha_1 \ldots \alpha_k$

$comm(\beta_1) \ldots comm(\beta_k)$

$V(\alpha_1, \beta_1, \ldots, \alpha_k, \beta_k)$?

= accept



$\alpha_1 \ldots \alpha_k$

$\gamma_1 \ldots \gamma_k$

$$L'_{SVS} = \left\{ (\alpha_1 \ldots \alpha_k, \gamma_1 \ldots \gamma_k) \mid \exists \beta_i \; \forall i : \gamma_i = comm(\beta_i) \wedge S_i \right.$$

$$\left. V(\alpha_1, \beta_1, \ldots \alpha_k, \beta_k) = acc \right\}$$

PZK with aux. information

(P, V) is PZK with auxiliary information if $\forall$ PPT V^*

$\exists$ PPT S^* s.t.

1) $\forall x$ and $\forall z$, $S^*(x, z)$ outputs $\perp$ w.p. $\leq 1/2$

2) $\forall x \in L$ and $\forall z$, $S^*(x, z)$ condition on not being $\perp$ is distributed identically to $\text{View}^P_{V^*(z)}(x)$

$P \quad x \quad V^*(z)$

$\Rightarrow$

Statistical Distance bet. Distributions

D_0, D_1 over domain X

$$\Delta(D_0, D_1) = \max_{S \subseteq X} \left(D_0(S) - D_1(S) \right)$$

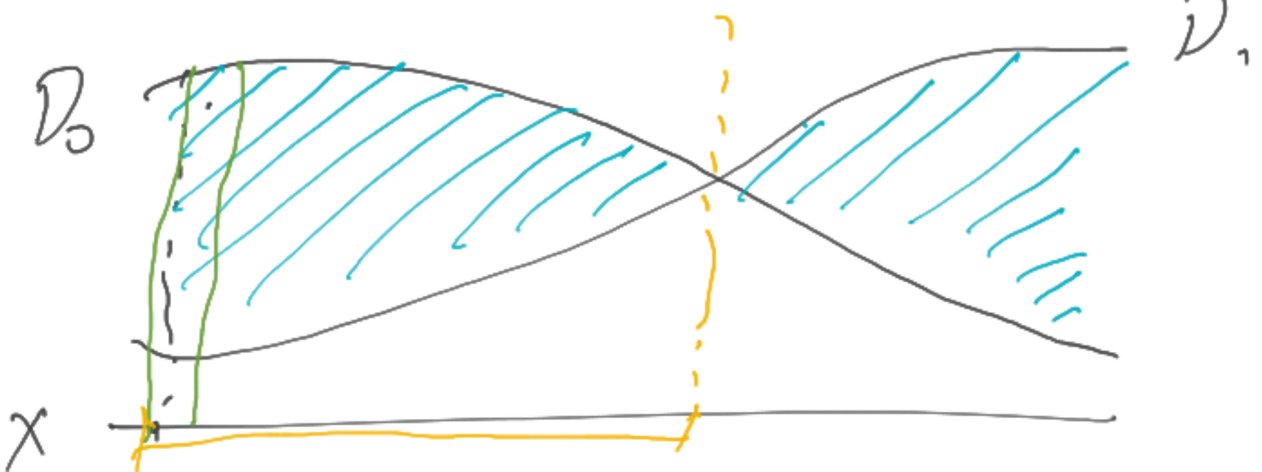
$$D_0(S) = \Pr_{D_0}[S \text{ happens}] \equiv \Pr_{x \leftarrow D_0}[x \in S] = \sum_{x \in S} D_0(x)$$

$$\Delta(D_0, D_1) = \frac{1}{2} \sum_x |D_0(x) - D_1(x)|$$

$\Delta(D, D) = 0$

if D_0 and D_1 are disjoint

$\Delta(D_0, D_1) = 1$



$$\mathrm{Adv}_{A}^{D_0,D_1} = \left| \Pr_{x \leftarrow D_0}[A(x)=1] - \Pr_{x \leftarrow D_1}[A(x)=1] \right| \leq \Delta(D_0,D_1)$$

$$\max_{A\ (\text{unbnd.})} \mathrm{Adv}_{A}^{D_0,D_1} = \Delta(D_0,D_1)$$

$$\Delta((X_0,X_1),(Y_0,Y_1)) \geq \Delta(X_0,Y_0) \text{ and } \Delta(X_1,Y_1)$$

$$\Delta((X_0,X_1),(Y_0,Y_1)) \leq \Delta(X_0,Y_0) + \mathop{E}_{x \leftarrow X_0}\left[\Delta(X_1|_{X_0=x}, Y_1|_{Y_0=x})\right]$$

$$\leq \Delta(X_0,Y_0) + \Delta(X_1,Y_1) \quad \text{if } \begin{array}{l} X_0 \text{ ind. of } X_1 \\ Y_0 \text{ ind. of } Y_1 \end{array}$$

D_0, D_1 over X

$$\Pr_{x \leftarrow D_1}[E(x) \text{ happens}] \leq \Pr_{x \leftarrow D_0}[E(x) \text{ happens}] + \Delta(D_0, D_1)$$

$$\Pr_{x \leftarrow D_1}[E(x) \text{ happens}] \geq \Pr_{x \leftarrow D_0}[E(x) \text{ happens}] - \Delta(D_0, D_1)$$

Statistical Zero Knowledge

(P, V) is SZK if $\forall$ PPT V^* $\exists$ PPT S_{V^*} s.t.

$\forall x \in L$:

$$S_{V^*}(x) \approx_s View^P_{V^*}(x)$$

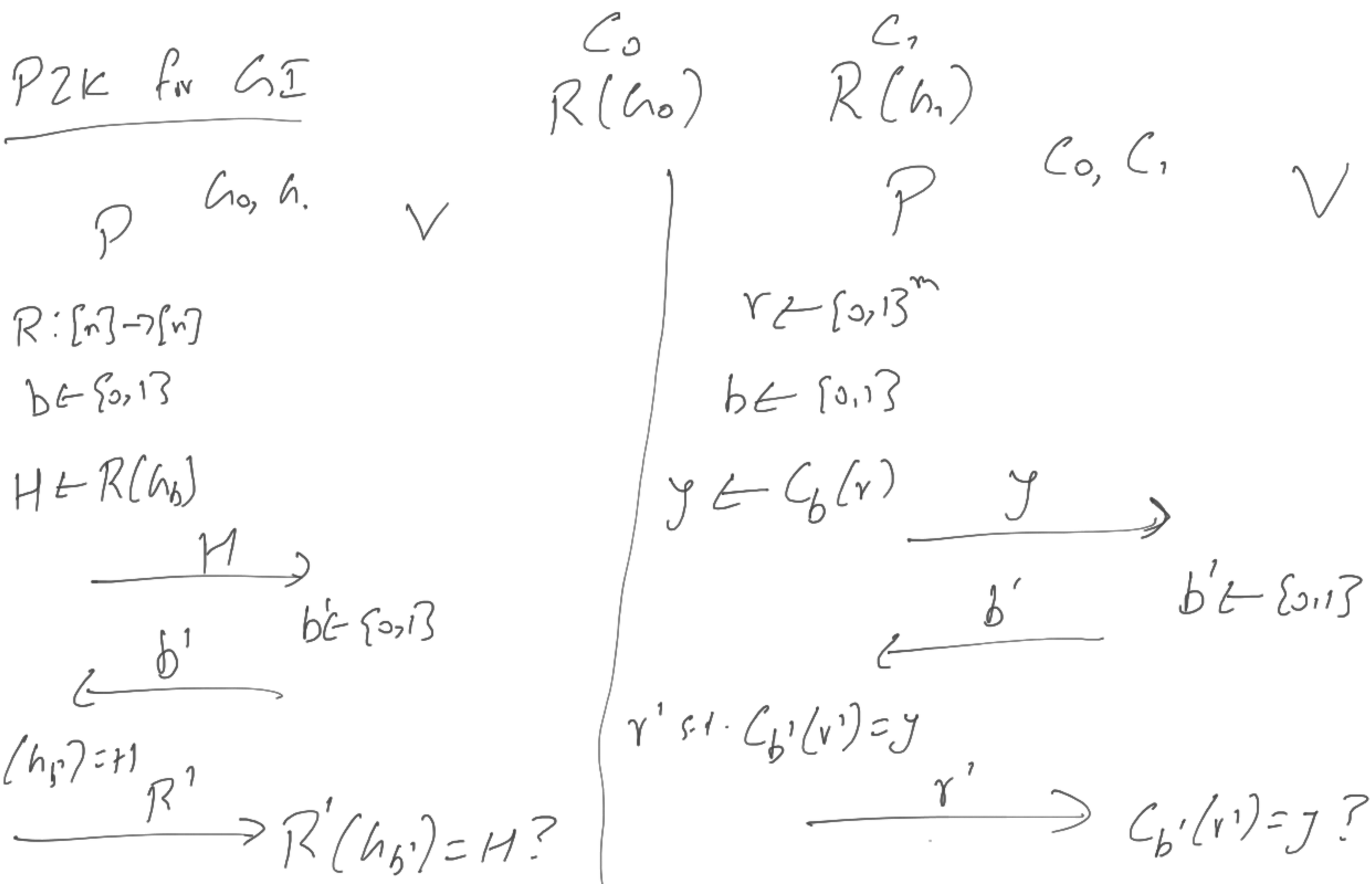
$$\downarrow \qquad\qquad \downarrow$$

$$\{S_{V^*}(x, 1^\lambda)\}_{\lambda \in \mathbb{N}} \qquad \{View^{P(1^\lambda)}_{V^*(1^\lambda)}(x)\}_{\lambda \in \mathbb{N}}$$

$$PZK \subseteq SZK \subseteq CZK$$

$$SZK \subseteq AM \cap coAM$$

PZK for GI


C_0
C_1
$R(G_0)$
$R(G_1)$
P
G_0, G_1
V
$R : [n] \to [n]$
$b \leftarrow \{0,1\}$
$H \leftarrow R(G_b)$
H
$b' \in \{0,1\}$
b'
$R'(G_{b'}) = H$
R'
$R'(G_{b'}) = H$?
$r \leftarrow \{0,1\}^m$
$b \leftarrow \{0,1\}$
$y \leftarrow C_b(r)$
y
$b' \leftarrow \{0,1\}$
b'
$r' s.t. C_{b'}(r') = y$
r'
$C_{b'}(r') = y$?

$C_0, C_1 : \{0,1\}^m \to \{0,1\}^n$

D_{C_0}

Distrib of $C_0(r)$ when $r \leftarrow \{0,1\}^m$

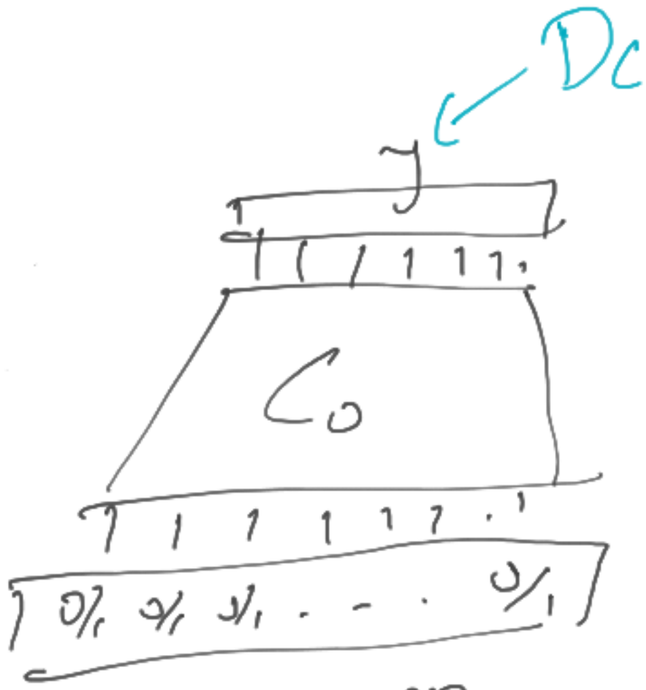
Distribution of $C_1(r)$ when $r \leftarrow \{0,1\}^m$

D_{C_1}

$$SC_Y = \{ (C_0, C_1) \mid \Delta(D_{C_0}, D_{C_1}) = 0 \}$$

$$SC_N = \{ (C_0, C_1) \mid \Delta(D_{C_0}, D_{C_1}) = 1 \}$$

in ranges of C_0 and C_1 are disjoint



$\Delta(C_0, C_1)$

$\Delta\left(\left[C_0(r) \mid r \leftarrow \{0,1\}^m \right), \left(C_1(r) \mid r \leftarrow \{0,1\}^m \right) \right)$

D_{C_0}

D_{C_1}

$$SC_r^{\beta} = \{(C_0, C_1) \mid \Delta(D_{C_0}, D_{C_1}) \leq \beta\}$$

$$SC_N^{\beta} = \{(C_0, C_1) \mid \Delta(D_{C_0}, D_{C_1}) = 1\}$$

$C_b : \{0,1\}^m \to \{0,1\}^n$

C_0, C_1

P

r, b

$y \leftarrow C_b(r)$

y →

← b'

$C_{b'}(r') = y$

r' →

$C_{b'}(r') = y$?

V

Comp:

$E(y) = \exists r' : C_1(r') = y$

$$Pr_{y \leftarrow D_{C_0}}[E(y)] \geq Pr_{y \leftarrow D_{C_1}}[E(y)] - \Delta(D_{C_0}, D_{C_1})$$

$$\geq 1 - \beta$$

Soundness: same as before

ZK: for any V^*, S_{V^*} :

1. Samples $r \leftarrow \{0,1\}^m$, $b \leftarrow \{0,1\}$, r_{V^*}
2. Compute $y \leftarrow C_b(r)$
3. Compute $b' \leftarrow V^*(C_0, C_1, y; r_{V^*})$
4. If $b \neq b'$, fail
5. Else output $(r_{V^*}, y, b, r, \pi(\dots))$

fail w.p. $\leq 1/2$

these dists. are same

$$\text{View}^P_{V^*} = (r_{V^*}, y, b', r', \pi(\dots))$$

$$\left| \Pr[b'=1 \mid b=0] - \Pr[b'=1 \mid b=1] \right| \leq \beta$$

(Dist. of $b' \mid b=0$) (Dist. of $b' \mid b=1$)

$$\Pr[b = b'] = \Pr[b' = 1 \mid b = 1] \cdot \Pr[b = 1]$$
$$+ \Pr[b' = 0 \mid b = 0] \cdot \Pr[b = 0]$$