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

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

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

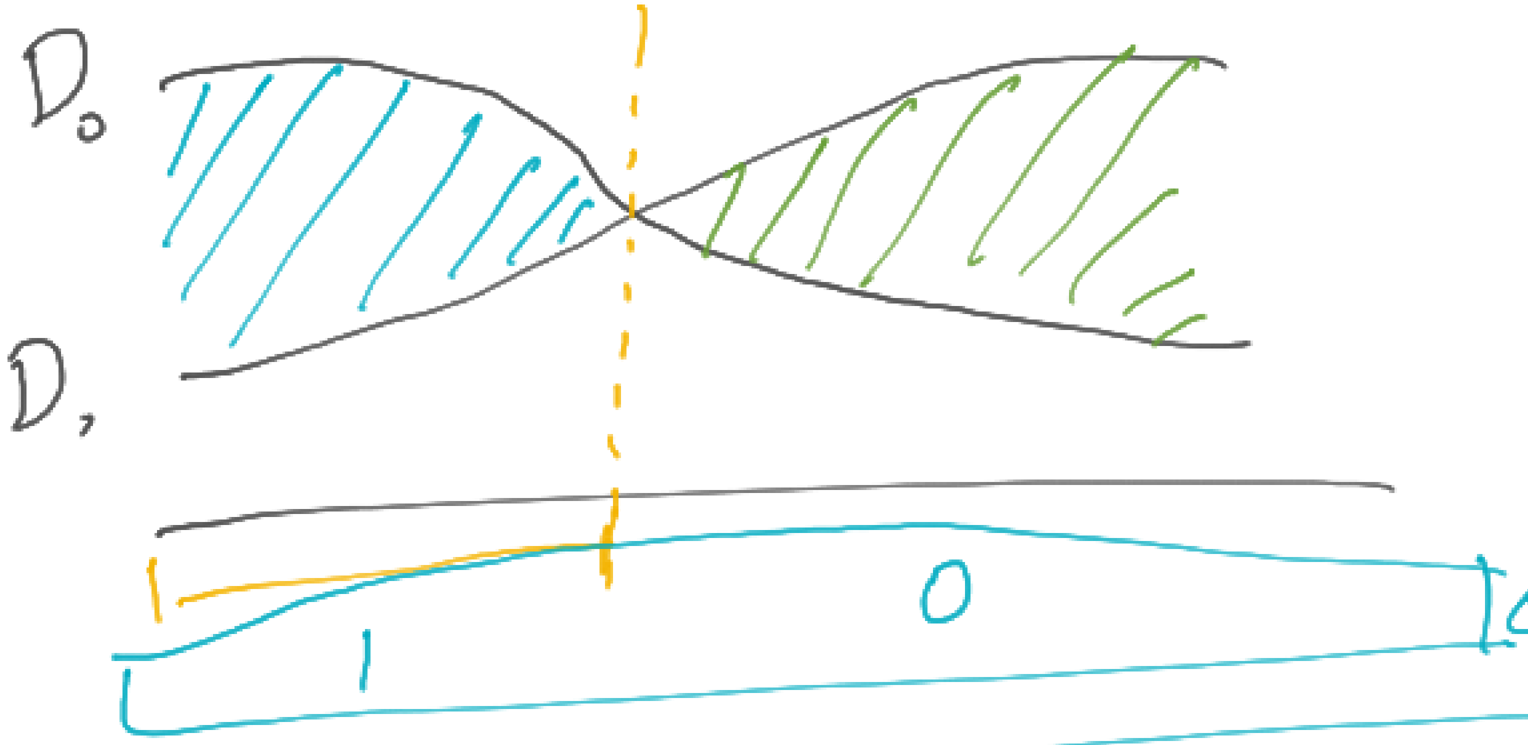
Completeness error : $\beta/2$

Soundness error : $1/2$

Zero-knowledge error: $\beta + \text{negl}(\lambda)$

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

$$= \max_A \mathrm{Adv}_A^{D_0, D_1}$$



$$A_{D_0, D_1}(x) = \begin{cases} 1 & \text{if } D_0(x) > D_1(x) \\ 0 & \text{else} \end{cases}$$

$$\Delta((X_0, Y_0), (X_1, Y_1)) \geq \max\left[\Delta(X_0, X_1), \Delta(Y_0, Y_1)\right]$$

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

$$\leq \Delta(X_0, X_1) + \Delta(Y_0, Y_1)$$ if X_0 indep. of Y_0, X_1 indep. of Y_1

$SC^{\beta} \longrightarrow SC^{2^{-\lambda}}$ in poly(λ) time

$D_0, D_1 \longrightarrow D_0^{\oplus n}, D_1^{\oplus n}$

$\Delta(D_0, D_1) = \delta \qquad \Delta(D_0^{\oplus n}, D_1^{\oplus n}) = \delta^n$

$(C_0, C_1) \in SC_Y^{\beta} \quad \Delta(D_{C_0}, D_{C_1}) \leq \beta \quad \Delta\left(D_{C_0}^{\oplus n}, D_{C_1}^{\oplus n}\right) \leq \beta^n$

$(C_0, C_1) \in SC_N^{\beta} \quad \Delta(D_{C_0}, D_{C_1}) = 1 \quad \Delta\left(D_{C_0}^{\oplus n}, D_{C_1}^{\oplus n}\right) = 1$

$D_b^{\oplus n}$: (D_0, D_1, n)

- Sample random bits $b_1, \ldots, b_n \leftarrow \{0,1\}$ s.t. $b_1 \oplus \cdots \oplus b_n = b$
- Sample $\forall i \in [n]$: $x_i \leftarrow D_{b_i}$
- Output $(x_1, \ldots, x_n)$

XOR Lemma: $\Delta\left(D_0^{\oplus n}, D_1^{\oplus n}\right) = \Delta(D_0, D_1)^n$

$D_b^{\otimes n}$: (D_0, D_1, b)

- Sample $\forall i \in [n]$: $x_i \leftarrow D_b$
- Output $(x_1, \ldots, x_n)$

$$1 - 2^{-\frac{n \Delta(D_0, D_1)^2}{2}} \leq \Delta\left(D_0^{\otimes n}, D_1^{\otimes n}\right) \leq n \cdot \Delta(D_0, D_1)$$

Polarisation Lemma [Sahai-Vadhan '00]

For any $\alpha, \beta \in [0,1]$ s.t. $\alpha^2 > \beta$

$$(D_0, D_1) \longrightarrow (D_0', D_1') \quad \text{in poly}(\lambda) \text{ time}$$

$$\Delta(D_0, D_1) \geq \alpha \implies \Delta(D_0', D_1') > 1 - 2^{-\lambda}$$

$$\Delta(D_0, D_1) \leq \beta \implies \Delta(D_0', D_1') < 2^{-\lambda}$$

$\alpha, \beta \in [0,1] \quad \alpha > \beta$

$$SC_Y^{\beta,\alpha} = \{ (c_0, c_1) \mid \Delta(D_{c_0}, D_{c_1}) \leq \beta \} = SD_N^{\alpha,\beta}$$

$$SC_N^{\beta,\alpha} = \{ (c_0, c_1) \mid \Delta(D_{c_0}, D_{c_1}) \geq \alpha \} = SD_Y^{\alpha,\beta}$$

(G_0, G_1)

P   V

$b \leftarrow \{0,1\}$

$R \leftarrow$ random relabelling

$H \leftarrow R(G_b)$

$\xleftarrow{\quad H \quad}$

if $H \equiv G_0$

$b' = 0$

else $b' = 1$

$\xrightarrow{\quad b' \quad}$

$b = b'$?

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

P   V

$b \leftarrow \{0,1\}$

$r \leftarrow \{0,1\}^m$

$y \leftarrow C_b(r)$

$\xleftarrow{\quad y \quad}$

if $D_{C_0}(y) > D_{C_1}(y)$

$b' = 0$

else $b' = 1$

$\xrightarrow{\quad b' \quad}$

$b = b'$?

Completeness: $\Delta(D_{C_0}, D_{C_1}) \geq \alpha$

$$\Pr[b' = b] = \frac{1}{2} \cdot \Pr[b' = 0 \mid b = 0] + \frac{1}{2} \cdot \Pr[b' = 1 \mid b = 1]$$

$$= \frac{1}{2} + \frac{1}{2} \cdot \left(\Pr[b' = 0 \mid b = 0] - \Pr[b' = 0 \mid b = 1] \right)$$

$$\Pr_{y \leftarrow D_{C_0}}[P(y) = 0] - \Pr_{y \leftarrow D_{C_1}}[P(y) = 0]$$

$$= Adv_P^{D_0, D_1} = \Delta(D_{C_0}, D_{C_1})$$

$$\geq \frac{1}{2} + \frac{\alpha}{2}$$

Soundness: $\Delta(D_{C_0}, D_{C_1}) \leq \beta$

$$\Pr[b = b'] = \frac{1}{2} + \frac{\mathrm{Adv}_P^{D_0, D_1}}{2} \leq \frac{1}{2} + \frac{\Delta(D_{C_0}, D_{C_1})}{2}$$

$$\leq \frac{1}{2} + \frac{\beta}{2}$$

$$\mathrm{View}_V^P(C_0, C_1) = ((r, b), y, b', out)$$

S2K:

$S(C_0, C_1)$: 1. Sample $r \leftarrow \{0,1\}^m$, $b \leftarrow \{0,1\}$

2. Compute $y \leftarrow C_b(r)$

3. Output $((r,b), y, b, accept)$

$$\mathrm{View}_V^P = ((R, B), Y, B', O)$$

$$S = ((R_S, B_S), Y_S, \underset{\underset{\textstyle B_S}{\shortparallel}}{B'_S}, O_S)$$

$$\Delta\Big((R, B, Y, B', O), (R_S, B_S, Y_S, B_S, O_S)\Big)$$

$$\le \Delta\Big((R, B, Y), (R_S, B_S, Y_S)\Big) = 0$$

$$+ \mathop{E}_{(r,b,y) \leftarrow (R,B,Y)} \Big[\Delta\Big(\underbrace{(B', O) \,|\, (R,B,Y) = (r,b,y)}, \underbrace{(B_S, O_S) \,|\, (R_S, B_S, Y_S) = (r,b,y)}_{\simeq\, (b,\ \text{accept})} \Big) \Big]$$

$$(B', O) = \begin{cases} (b, \text{accept}) & \text{with prob. } p(r,b,y) \\ (1-b, \text{reject}) & \text{with prob. } 1 - p(r,b,y) \end{cases}$$

$$= \mathop{E}_{(r,b,y)} \big[1 - p(r,b,y) \big] = 1 - E\big[p(r,b,y) \big]$$

$$= 1 - \mathop{E}_{(r,b,y) \leftarrow (R,B,Y)} \left[p(r,b,y) \right] = 1 - \mathop{E}_{(r,b,y)} \left[\Pr [B' = b] \right]$$

$$= 1 - \Pr [B' = B] \leq 1 - \left(\frac{1}{2} + \frac{\alpha}{2} \right) = \frac{1}{2} - \frac{\alpha}{2}$$