Вероятн. коммун. протоколы π, R, R_A, R_B

μ - распр X, Y

$$IC_\mu^{int}(\pi) = I(X : M(Y,R)) + I(Y : M | X,R)$$

$$IC_\mu^{int}(\pi) \le \underset{\mu,R,R_A R_B}{E}[|M|]$$

$$NDISJ : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$

$$NDISJ(x,y) = \bigvee_{i=1}^{n} (x_i \wedge y_i)$$

A и B две распр с носителем в U

U конечно

$$\Delta(A,B) = \max_{V \subseteq U} \left| Pr[A \in V] - Pr[B \in V] \right| =$$

$$= \frac{1}{2} \sum_{v \in U} \left| Pr[A = v] - Pr[B = v] \right| = \frac{1}{2} \|A - B\|_1$$

Св-ва Δ:

1) $\Delta(A,C) \le \Delta(A,B) + \Delta(B,C)$

2) $A \times B$ ← конец B не завис. от A

$$\Delta(A \times C, B \times C) = \Delta(A,B)$$

3) $\Delta(A \times B, A' \times B') \le \Delta(A,A') + \Delta(B,B')$

Д-во $\Delta(A\times B, A'\times B') \le \Delta(A\times B, A'\times B) +$

$+ \Delta(A'\times B, A'\times B') = \Delta(A, A') + \Delta(B, B')$

4) $\Delta(AC, BC) = \underset{c}{E}\left[\Delta(A|_{C=c}, B|_{C=c})\right]$

5) $\Delta(AB, A\times B) = \underset{b}{E}\left[\Delta(A|_{B=b}, A)\right]$

Теорема (Нер-во Пинскера)

$$\Delta(AB, A\times B) \le \sqrt{\frac{I(A:B)\ln 2}{2}}$$

Теорема $\forall$ вероятн. ком. протокола, кот. исп. только публичные случ. биты) и вычисл. NP[SJ с вер-тью ошибки $\le \frac{1}{2} - \delta$ $\forall$ входе в худшем случае передаёт $\ge c\cdot\delta^2 n$ битов, где $c = \frac{2-\sqrt{2}}{\ln 2} \approx 0.845$

Д-во] есть вер. прот. в худшем случае передаёт ℓ битов. Дает прав. ответ с вер. $\ge \frac{1}{2} + \delta$.

μ - распр на (X, Y)

$\Pr_{\mu,R}[$ прот дает прав ответ $] \ge \frac{1}{2} + \delta$

$R \leftarrow \{0,1\}^*$

$\forall$ распр μ $\exists$ детерм протокол T длины $\le \ell$, кот. на случ. вх $\sim\mu$ дает верный ответ с вер-тью $\ge \frac{1}{2} + \delta$.

A и B $\quad$ $\bar{A}$ и $\bar{B}$ $\quad$ распр на $\{0,1\}$

- $\Pr[A \wedge B = 1] = \frac{1}{2}$
- $\Pr[\bar{A} \wedge \bar{B} = 1] = 0$

Распред. μ:

$i \leftarrow [n]$ случайно

$X = \tilde{A} \ldots \tilde{A}\ A\ \hat{A} \ldots \hat{A}$

$Y = \tilde{B} \ldots \tilde{B}\ B\ \hat{B} \ldots \hat{B}$

i

Π – дет. протокол для NDISJ выс. $\leq \ell$

$$\Pr_{X,Y \sim \mu} [\Pi(X,Y) = NDISJ(X,Y)] \geq \frac{1}{2} + \delta$$

Π' – протокол для конъюнкции

(A,B)

a – вход Алисы

b – вход Боба

$i \leftarrow [n]$ – случайное

$x = u\ a\ v'$

$y = u'\ b\ v$

u: $i-1$ бит; v: $n-i$ бит

u и v выбираются из публичных битов.

v' выб. Алиса из ее приватных битов

u' – Боб

$\hat{A} \mid \hat{B} = b$

Выдает ответ $\Pi(X,Y)$.

$$\Pr[\Pi'(A,B) = A \wedge B] \geq \frac{1}{2} + \delta$$

Проверим

$$IC_{A,B}(\Pi') \leq \frac{\ell}{n}$$

$\hat{A} \ldots A \ldots \hat{A}$

$\hat{B} \quad B \ldots \hat{B}$

I – случ. вел. на выбор i

$\mu \quad X, Y$

$\tilde{\mu} \quad \tilde{X}, \tilde{Y}$

$\tilde{A} \ldots \hat{A}$

$\tilde{B} \ldots \hat{B}$

$$IC_{A,B}(\Pi') = I(\tilde{X}_I : \tilde{M} \mid \tilde{Y}_I, X_{<I}, \tilde{Y}_{>I}, I) + I(\tilde{Y}_I : \tilde{M} \mid \tilde{X}_I, X_{<I}, \tilde{Y}_{>I}, I).$$

$\leq$

$$I(\tilde{X}_I : \tilde{M} \mid \tilde{Y}_I, \tilde{X}_{<I}, \tilde{Y}_{>I}, I) =$$

$$= \frac{1}{n} \sum_{i=1}^{n} I(\tilde{X}_i : \tilde{M} \mid \tilde{Y}_i, \tilde{X}_{<i}, \tilde{Y}_{>i}) =$$

$$= \frac{1}{n} \sum_{i=1}^{n} I(\tilde{X}_i : \tilde{M} \mid \tilde{Y}_{\geq i}, \tilde{X}_{<i}) \leq$$

$$\leq \frac{1}{n} \sum_{i=1}^{n} I(\tilde{X}_i : \tilde{M} \mid \tilde{Y}, \tilde{X}_{<i}) =$$

неявно $\tilde{Y}_{<i}$ незав. с $\tilde{X}_i$ при усл. $\tilde{Y}_{\geq i}, \tilde{X}_{<i}$

$$= \frac{1}{n} I(\tilde{X} : \tilde{M} \mid \tilde{Y})$$

$$\leq \frac{1}{n} I(\tilde{X} : \tilde{M} \mid \tilde{Y}) +$$

$$+ \frac{1}{n} I(\tilde{Y} : \tilde{M} \mid \tilde{X}) =$$

$$= \frac{1}{n} IC_{\mu}(\pi) \leq \frac{\ell}{n}$$

$$\left[\begin{array}{l} \tilde{\pi}: \\ \Pr[\tilde{\pi}(A,B) = A \wedge B] \geq 1/2 + \delta \\ IC_{A,B}(\tilde{\pi}) \leq \ell/n \end{array} \right]$$

- A и B неравны
- $\Pr[A \wedge B = 1] = 1/2$
- $\Pr[\tilde{A} \wedge \tilde{B} = 1] = 0$
- $\Pr[\tilde{A} = 0] = \Pr[\tilde{B} = 0] > 0$
- $A|_{B=0}$ и $\tilde{A}|_{\tilde{B}=0}$ одинаковые
  $B|_{A=0}$ и $\tilde{B}|_{\tilde{A}=0}$

$$\Pr[\tilde{A} = 0] = \Pr[\tilde{B} = 0] = \frac{1}{1+\sqrt{2}} = 2 - \sqrt{2}$$

A и B неч	$\Pr[A=1] = \Pr[B=1] =$	$\frac{1}{\sqrt{2}}$
$(\tilde{A}, \tilde{B})$	$(0,0)$	$(0,1)$ $(1,0)$
	$\frac{1-\sqrt{2}}{1+\sqrt{2}}$	$\frac{\sqrt{2}}{1+\sqrt{2}}$ $\frac{\sqrt{2}}{1+\sqrt{2}}$

Лемма $\Pr[\pi'(A,B) = A \wedge B] \le \frac{1}{2} + \sqrt{IC^{(\pi')}_{\tilde{A},\tilde{B}}/d}$

$d = \frac{2-\sqrt{2}}{\ln 2}$ $\sqrt{\frac{\varepsilon}{nd}} \ge \delta$ $\varepsilon \ge \delta^2 n d$

Д-во леммы

Докажем для случая, когда π' не имеет общих сущ. битов.

$$IC_{\tilde{A},\tilde{B}}(\pi') = I(\tilde{A} : \tilde{M} | \tilde{B}) + I(\tilde{B} : \tilde{M} | \tilde{A})$$

$$= I(\tilde{A} : \tilde{M} | \tilde{B}=0) \cdot \Pr[\tilde{B}=0] +$$

$$+ I(\tilde{B} : \tilde{M} | \tilde{A}=0) \cdot \Pr[\tilde{A}=0] =$$

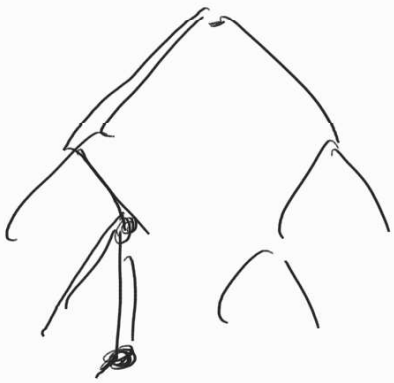
$$= \left(I(\tilde{A} : \tilde{M} | \tilde{B}=0) + I(\tilde{B} : \tilde{M} | \tilde{A}=0)\right) \cdot \left(2-\sqrt{2}\right)$$

$$I(\tilde{A} : \tilde{M} | \tilde{B}=0) + I(\tilde{B} : \tilde{M} | \tilde{A}=0) = \frac{IC^{(\pi')}_{\tilde{A},\tilde{B}}}{2-\sqrt{2}}$$

$$I(A:M \mid B=0) + I(B:M \mid A=0) =$$

$$= IC_{\vec{A},\vec{B}}(\pi') \cdot \frac{1}{2-\sqrt{2}}$$

Утв. A и B независимы при усл. $M=m$.



$$U \in \mathcal{U}$$

$$A, R_{AR} \in U$$

$$B, R_B \in V$$

$$\Pr[A=a \mid B=b, M=m] =$$

$$= \Pr[A=a \mid B=b, (A,R_A)\in U, (B,R_B)\in V] =$$

$$= \Pr[A=a \mid (A,R_A)\in U] =$$

$$= \Pr[A=a \mid (A,R_A)\in U, (B,R_B)\in V]$$

$$= \Pr[A=a \mid M=m]$$

$$\Pr_{A,B}\left[\pi'(A,B) = A \wedge B\right] = \mathop{E}_{m} \Pr\left[\pi'(A,B) = A\wedge B \,\middle|\, M=m\right]$$

$$= \mathop{E}_{m}\left[\Pr\left[A\wedge B = \text{пометки места } m \,\middle|\, M=m\right]\right]$$

$$\le \frac{1}{2} + \mathop{E}_{m}\left[\Delta\left((A,B)|_{M=m}, (A,B)\right)\right]$$

$$\Delta\left((A,B)|_{M=m}, (A,B)\right) =$$

$$= \Delta\left(A|_{M=m} \times B|_{M=m}, A\times B\right) \le$$

$$\le \underbrace{\Delta\left(A|_{M=m}, A\right)}_{d_m} + \underbrace{\Delta\left(B|_{M=m}, B\right)}_{e_m}$$

Утв.

$$\mathop{E}_{m}\{d_m\} \le \sqrt{I(A:M\,|\,B=0)\frac{\ln 2}{2}}$$

$$\mathop{E}_{m}\{e_m\} \le \sqrt{I(B:M\,|\,A=0)\cdot\frac{\ln 2}{2}}$$

$$\mathop{E}_{m}\left[d_m + e_m\right] \le \sqrt{\left(I(A:M\,|\,B=0) + I(B:M\,|\,A=0)\right)\ln 2}$$

$$\le \sqrt{IC_{A,B}(\pi')\frac{\ln 2}{2-\sqrt{2}}}$$

Д-во утв-ие $\quad \sqrt{x}+\sqrt{y} \quad \sqrt{x+y}$

$$E[d_m] = \underset{m}{E}\left[\Delta\left(A|_{M=m}, A\right)\right] =$$

$$= \underset{m}{E}\left[\Delta\left(A|_{M=m,B=0}, A|_{B=0}\right)\right]$$

$$= \Delta\left((A,M)|_{B=0}, A|_{B=0} \times M|_{B=0}\right)$$

$$\leq \sqrt{\frac{I(A:M|B=0)\ln 2}{2}}$$