$$I(A,B:C) = I(A:C) + I(B:C|A)$$

$$I(X_1, X_2, \ldots X_n : C) = \sum_{i=1}^{n} I(X_i : C | X_{<i})$$

$I(A:B)$ $\quad$ $I(A:B|C)$

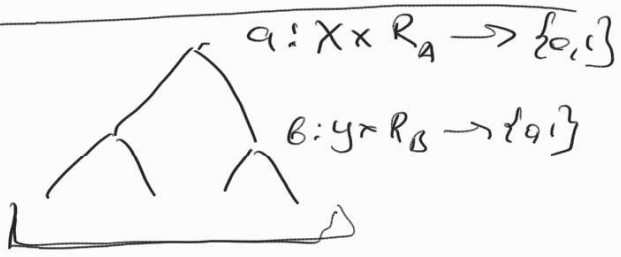
$= H(A) - H(A|B)$ $\quad$ $= H(A|C) - H(A|BC)$

Если A и C независ $\Rightarrow$ $I(A:B) \le I(A:B|C)$
B и C независ

Кон. протоколы

приватные случ. биты R_A, R_B

публичные случ. биты R



μ распр (X, Y)

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

M – послед-ть передаваемых битов в протоколе

$I(M,R:X|Y) = I(R:X|Y) + I(M:X|Y,R)$

$I(R:X|Y) = 0$

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

$$IC_\mu^{ext}(\Pi) = I(M, R : X, Y)$$

Теорема (1) $IC_\mu^{int}(\Pi) \le H(M|R)$

(2) Если протокол не исп. приватных сл. битов, то $IC_\mu^{ext} = H(M|R)$

(3) $H(M|R) \le$ средней длины сообщ.

Д-во (2) $IC_\mu^{ext}(\Pi) = I(M,R:X,Y) =$

$= I(R:X,Y) + I(M:X,Y|R) =$

$I(R:X,Y) = 0$

$= H(M|R) - H(M|X,Y,R)$ $\qquad H(X|Y=a)$

(3) $H(M|R) = E_r[H(M|R=r)]$

(1) $IC_\mu^{int}(\Pi) = I(M : X \mid Y, R) + I(M : Y \mid X, R) =$

$= \sum_i \left(I(M_i : X \mid Y, R, M_{<i}) + I(M_i : Y \mid X, R, M_{<i}) \right) =$

$= \sum_i E_{y,r} \left(\underline{I(M_i : X \mid Y, R{=}r, M_{<i}{=}u)} + \underline{I(M_i : Y \mid X, R{=}r, M_{<i}{=}u)} \right)$

$\leq \sum_i E_{y,r} \left[\max \{ H(M_i \mid Y, R{=}r, M_{<i}{=}u), H(M_i \mid X, R{=}r, M_{<i}{=}u) \} \right]$

$\leq \sum_i E_{y,r} \left[H(M_i \mid R{=}r, M_{<i}{=}u) \right] = \sum_i H(M_i \mid R, M_{<i}) =$

$= H(M \mid R)$.

Direct sum problem

$f : X \times Y \to Z$

$f^n(x_1, \dots, x_n, y_1, \dots, y_n) = f(x_1, y_1), f(x_2, y_2), \dots, f(x_n, y_n)$

$\Pr_{(x,y) \leftarrow \mu} [\Pi(x,y) \neq f(x,y)] \leq \varepsilon \quad \forall i \in [n]$

$\Pr_{(x,y) \leftarrow \mu^n} [\Pi'(x,y)_i \neq f(x_i, y_i)] \leq \varepsilon$

Теорема Π протокол, который вычисляет f^n для вх. распр. с μ^n

Тогда мы построим такой протокол Π':

- $IC_\mu^{int}(\Pi') \leq IC_{\mu^n}^{int}(\Pi)/n$
- если $\forall i \ \Pr_{(x,y) \leftarrow \mu^n} [\Pi(x,y)_i \neq f(x_i, y_i)] \leq \varepsilon$

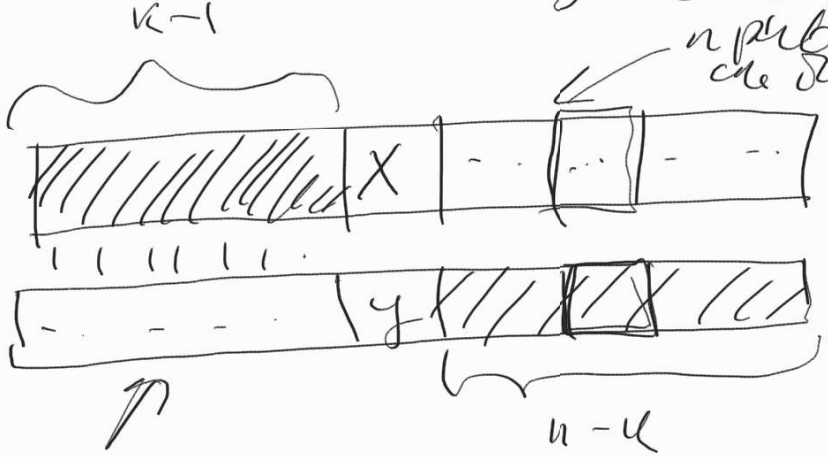
$\Rightarrow \Pr_{(x,y) \leftarrow \mu} [\Pi'(x,y) \neq f(x,y)] \leq \varepsilon$

2-bo

x y

Π' ——— равном. распр.

$K \leftarrow [n]$ (исп. публичные случ. биты)



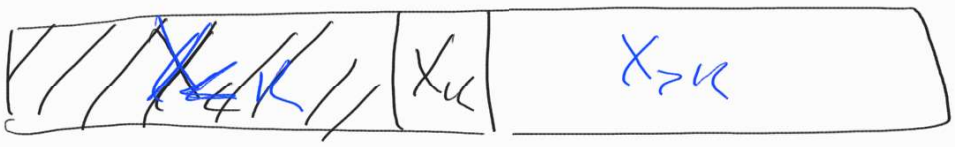
M

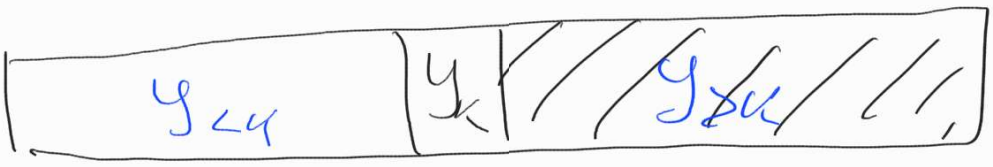
Алиса $\int_x^M \int_y^M$

Боб

$\int_x^M (y = b$

Выдаем ответ $\Pi(\bar{x}, \bar{y})$ K





$$IC_M(\Pi') = \underline{I}\left(X_K : M \mid Y_K, X_{<K}, Y_{>K}\right)$$

$$+ \underline{I}\left(Y_K : M \mid X_K, X_{<K}, Y_{>K}, K\right) =$$

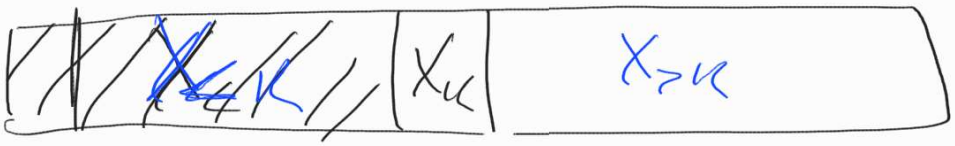
$$= \frac{1}{n} \sum_{k=1}^{n} \left(\underline{I}(\ldots \mid K=k) + \underline{I}(\ldots \mid K=k) \right)$$

$$= \frac{1}{n} \sum_{k=1}^{n} \left(\underline{I}(X_k : M \mid X_{<k}, Y_{\geq k}) + \right.$$

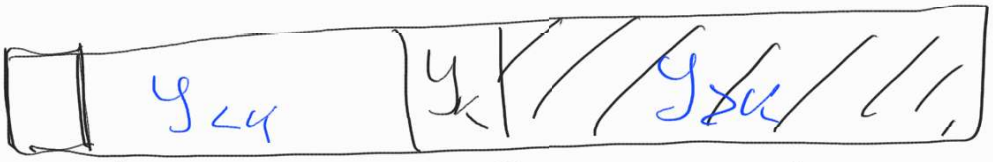
$$+ I(y_k : M \mid X_{\le k}, y_{>k})\Big) \le$$

$$\le \frac{1}{n}\sum_{k=1}^{n}\Big(I(X_k : M \mid X_{<k}, y) + I(y_k : M(X, y_{>k})\Big)$$

(=) Это корректно, если $y_{<k}$ и X_k независимы при условии $X_{<k}, y_{\ge k}$



$M|$



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

$= \frac{1}{n} IC_M^{int}(\Pi)$

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

$$= \bigvee_{i=1}^{n} (x_i \wedge y_i)$$

$$\Omega(n) \qquad \frac{\ell}{n} \ge c$$