Homomorphic Secret Sharing (HSS)

Share $(x) \longrightarrow x_0 \qquad x_1$

$f(x) \xleftarrow{\text{reconstruct}} y_0 \qquad y_1$

---

additive sharing

$\langle x \rangle = -x_0 + x_1$

$\langle y \rangle = -y_0 + y_1$

$\langle x+y \rangle = -(x_0+y_0) + (x_1+y_1)$

---

additive sharing

$\langle x \rangle = -x_0 + x_1$

El Gamal Encryptions

$\text{Enc}(k,x) = (h_1, h_2 = h_1^k g^x)$

$\text{Enc}(k,kx) = (\bar{h}_1, \bar{h}_2)$

$pk = (g, g^k)$

$\langle ky \rangle = -\bar{y}_0 + \bar{y}_1$

$\langle y \rangle = -y_0 + y_1$

$h_2^{\langle y \rangle} / h_1^{\langle ky \rangle} \quad h_2^{y_0} h_1^{\bar{y}_0} \quad h_2^{y_1} h_1^{\bar{y}_1}$

$\frac{h_2^{y_1} h_1^{\bar{y}_1}}{h_2^{y_0} h_1^{\bar{y}_0}} = \frac{h_2^{y}}{h_1^{ky}} = g^{xy}$

$\langle xy \rangle \quad \text{DDL}(z_0) \quad \text{DDL}(z_1)$

$\langle kxy \rangle = \text{DDL}(\bar{h}_2^{\langle y \rangle} / \bar{h}_1^{\langle ky \rangle})$

Note: We cannot get $\text{Enc}(k, xy)$ and $\text{Enc}(k, kxy)$.

So it only works for branching program f.

Paillier based DCR assumption

$pk = N = (2p'+1)(2q'+1) = p \cdot q$

$Enc(m) = r^N \cdot (1+N)^m = r^N (1+N)^m$.

additive share

$\langle x \rangle$: x_0 x_1

$Enc(x) = h^r (1+N)^{2m}$

$\varphi := (p-1)(q-1)$ $\langle \varphi y \rangle$: $\overline{y}_0$ $\overline{y}_1$

$\langle y \rangle$: y_0 y_1

$\frac{Enc(x)^{\overline{y}_1}}{Enc(x)^{y_0}} = Enc(x)^{\varphi y} = (1+N)^{2xy}$

$Enc(x)^{\langle \varphi y \rangle}$ $Enc(x)^{\overline{y}_0}$ $Enc(x)^{\overline{y}_1}$

$\langle 2\varphi xy \rangle$: $DDL(\overline{y}_0)$ $DDL(\overline{y}_1)$

$= r(1+N)^{w_0}$ $= z_0(1+N)^{2xy\varphi}$

$= r(1+N)^{w_0 + 2xy\varphi}$.

$r = z_0 \bmod N$

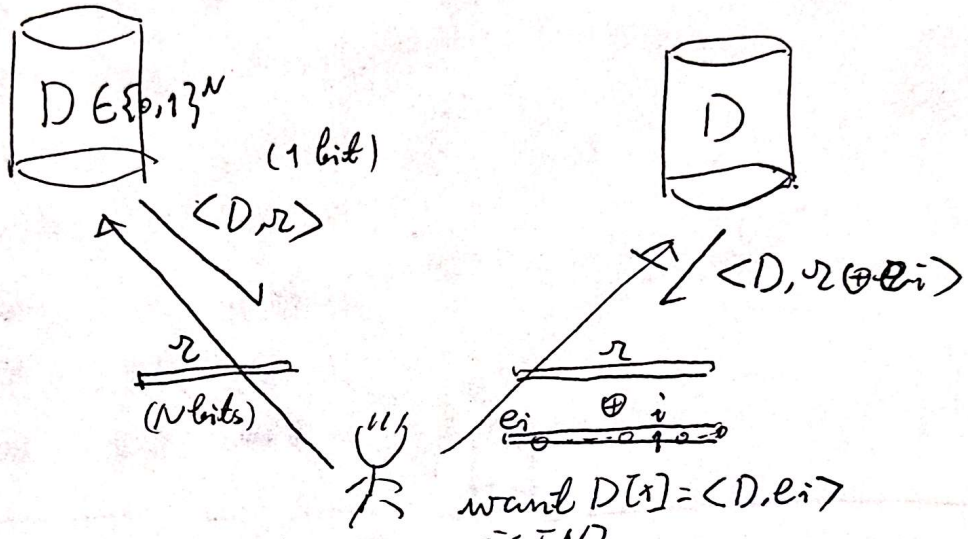
$= z_1 \bmod N$

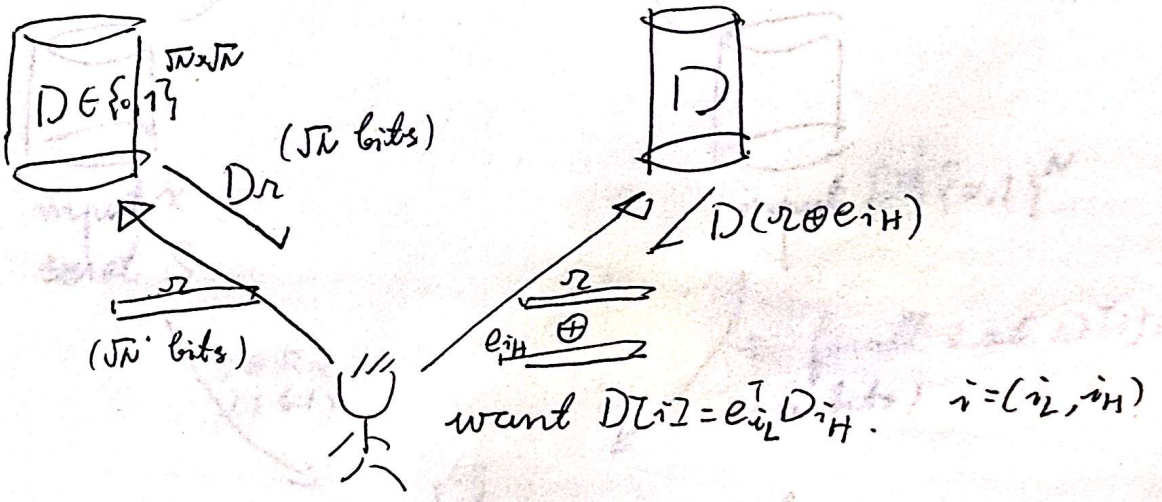
$\langle 2\varphi xy \rangle$: w_0 $w_0 + 2xy\varphi$.

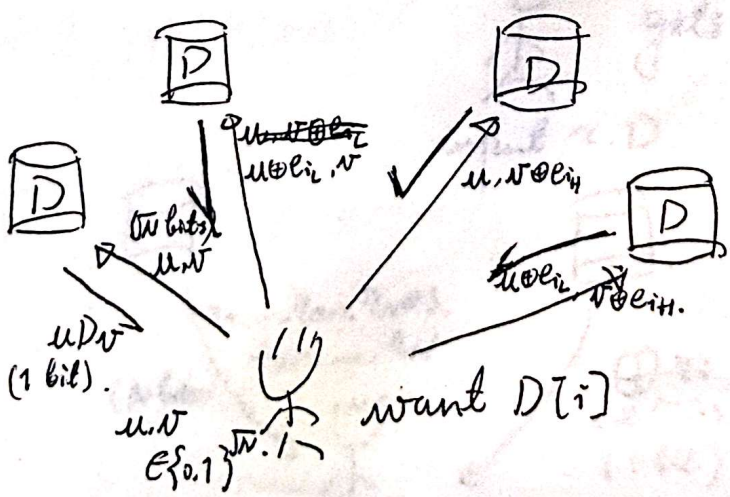
Claim: $\forall a \in \mathbb{Z}_{N^2}$, $a = (a \bmod N)(1+N)^{a'}$ for some a'

Information-Theoretic Cryptography.

- Private Information Retrieval (PIR)







4 servers

$u, v, w \in \{0,1\}^{\sqrt[3]{N}}$

(Best $2^{\sqrt{\log N \log\log N}}$)

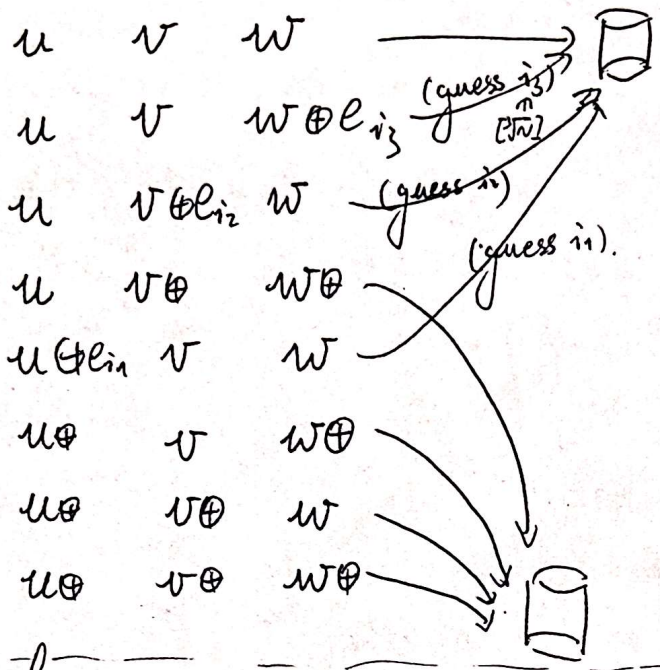
$\sqrt[3]{N}$

||

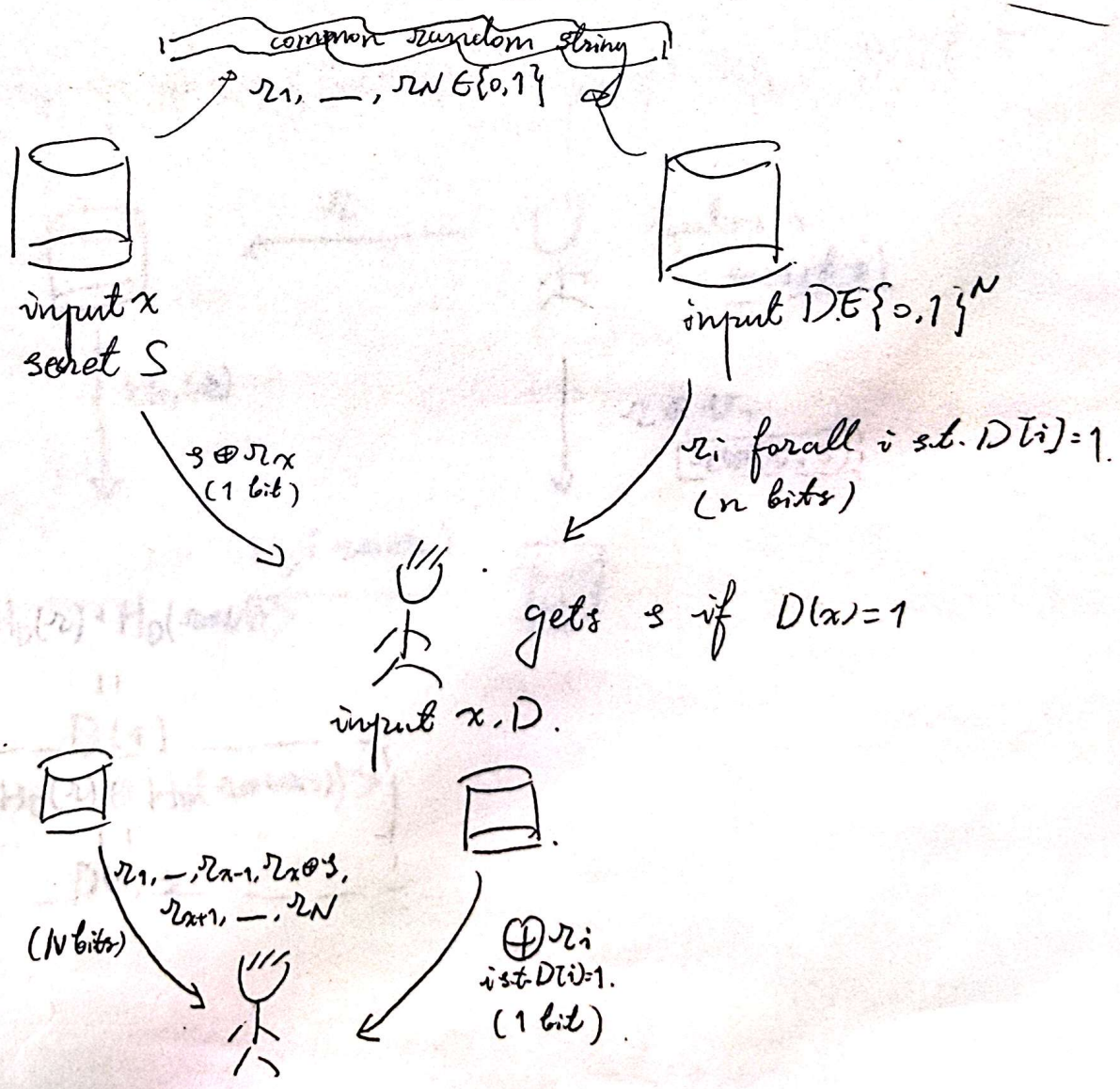
2PIR s.t.

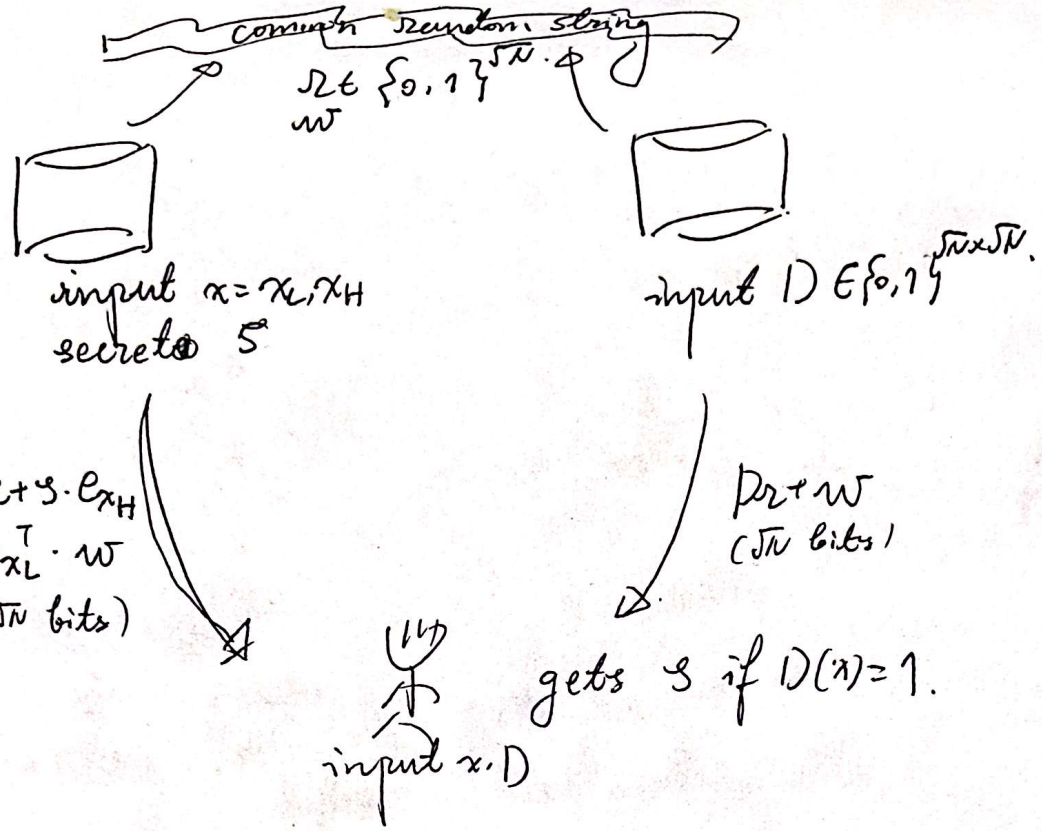
||

$\text{polylog}(N)$.



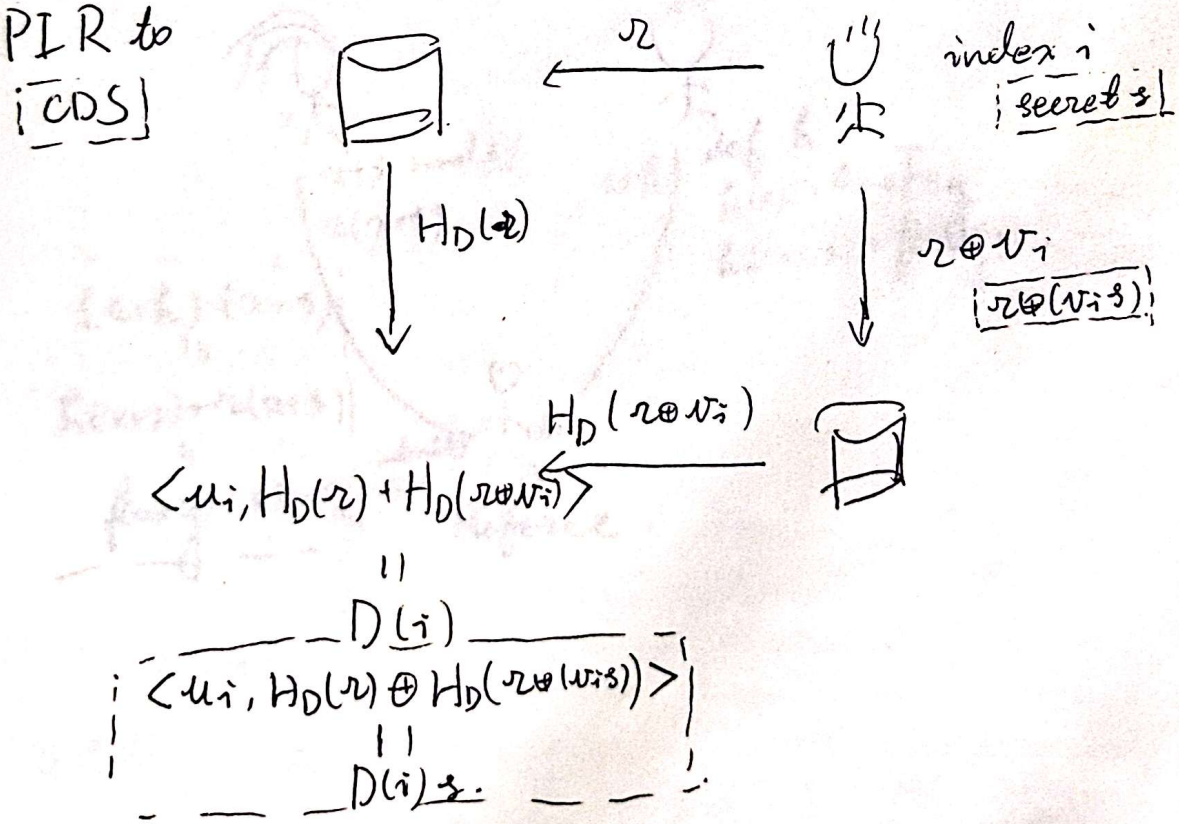
Conditional Disclosure of Secret (CDS)



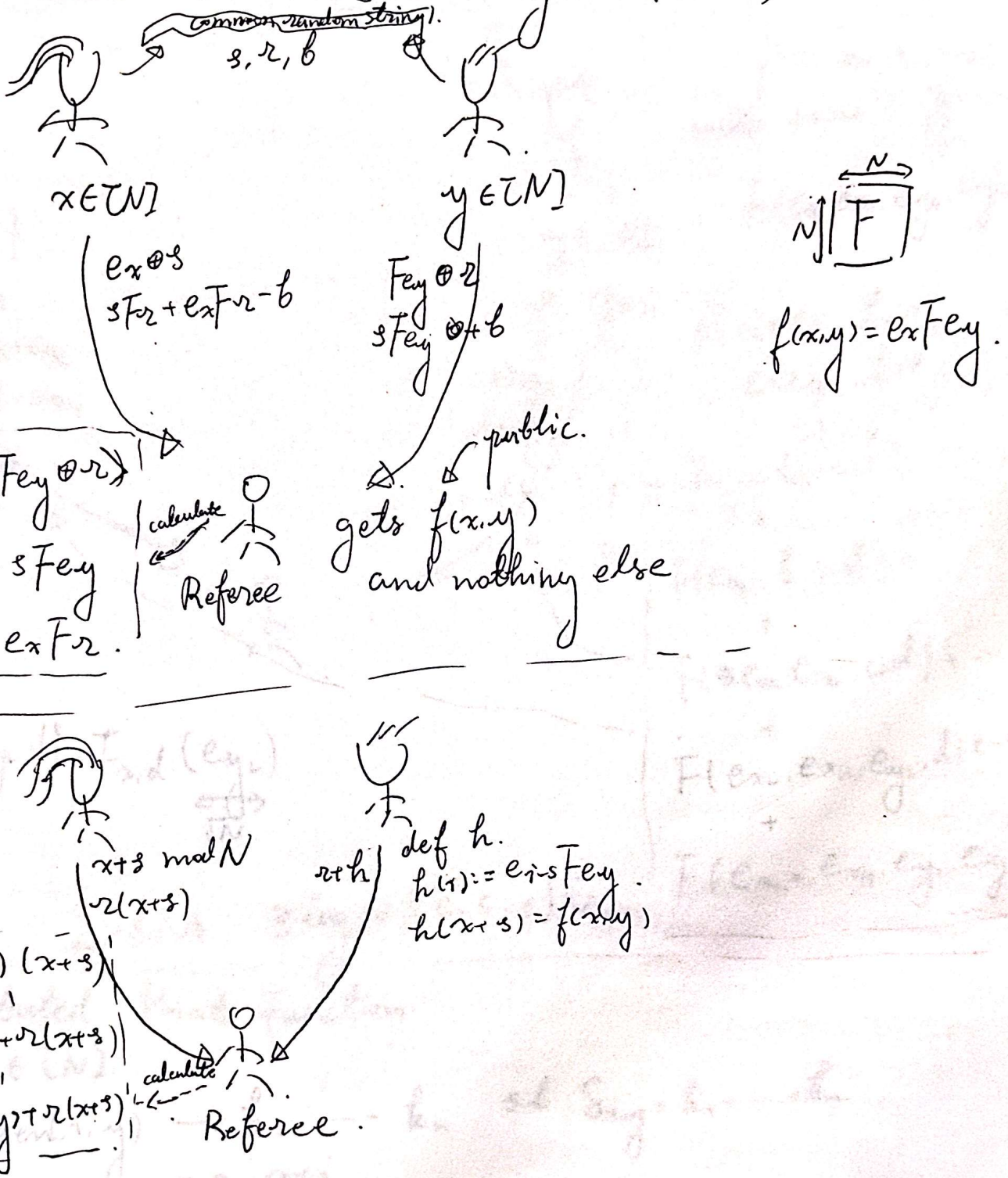


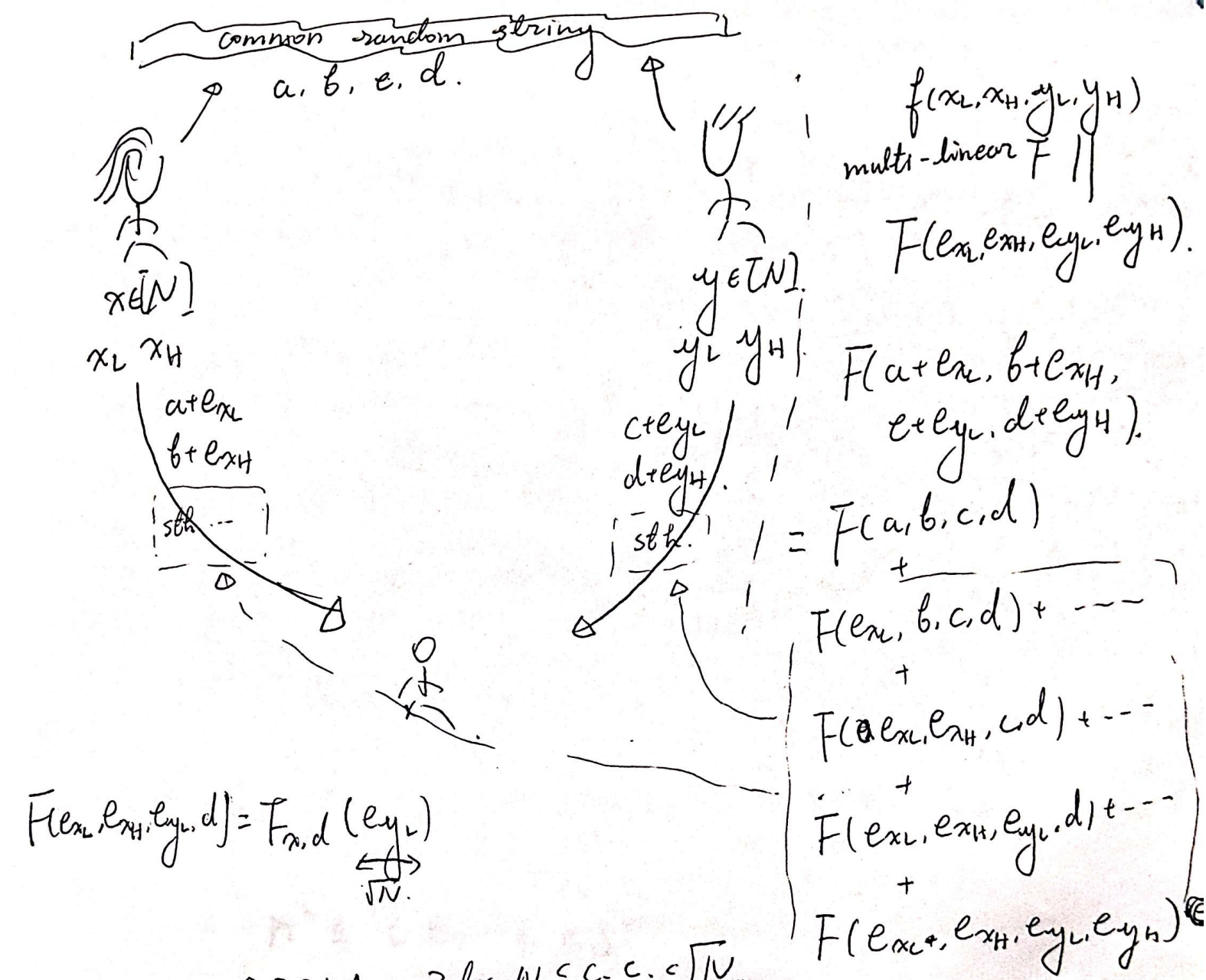
$$e_{x_L}^T \cdot w \oplus e_{x_L}(Dr + w) \oplus e_{x_L} D(r + s e_{x_H}) = s \cdot D(x)$$

PIR to [CDS]



– Private Simultaneous Messages (PSM)





2PSM $3\log N \le c.c. \le \sqrt{N}$.

- Distributed Point Function

$i \in [N]$

$Gen(i, y) \to k_1 \cdots k_n$ s.t. $\delta_{i,y} = k_1 + \cdots + k_n$.

$$\delta_{i,y}(x) := \begin{cases} 0 & x \neq i \\ y & x = i \end{cases}$$

4 PIR: index $i = (i_L, i_H)$

$k_1 = r \quad s$
$k_2 = r + e_{i_L} \quad s$
$k_3 = r \quad s + e_{i_H}$
$k_4 = r + e_{i_L} \quad s + e_{i_H}$

$r \otimes s$

4-server w/ c.c. $\sqrt{N}$.
DPF.
$\to e_i \otimes e_{i_H} = e_i$