Homomorphic Secret Sharing

	Alice	Bob
share(x) →	x_0	x_1
	↓	↓
reconstruct ←	y_0	y_1
$f(x)$ ←		

记：$\langle x \rangle$ 为 x 的 active share

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

尝试计算 $\langle xy \rangle$

记 ElGamel Encryption $Enc(k, x) = (h_1, h_2 = h_1^k g^x)$

$pk = (g, g^k)$ $\quad Enc(k, kx) = (\bar{h}_1, \bar{h}_2)$

	Alice	Bob
$\langle ky \rangle$	$\bar{y}_0$	$\bar{y}_1$
$\langle y \rangle$	y_0	y_1
$h_2^{\langle y \rangle}$	$h_2^{y_0}$	$h_2^{y_1}$
$\langle xy \rangle$	$DDL(h_2^{y_0} \cdot h_1^{\bar{y}_0})$	$DDL(h_2^{y_1} \cdot h_1^{\bar{y}_1})$

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

为使过程可持续，我们还需 kxy 的 share

因此还要有 $Enc(k, kx) = (\bar{h}_1, \bar{h}_2)$

Do the same thing with Pailliar Encryption:

* Pailliar based on DCR assumption.

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

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

(hard group)

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

---

active share $\langle x \rangle$ $\quad x_0 \quad x_1$

$\varphi = (p-1)(q-1)$ $\langle \varphi y \rangle \quad \varphi y_0 \quad \varphi y_1$ ←

$\langle y \rangle \quad y_0 \quad y_1$

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

$Enc(x)^{\langle y \rangle}$ $\quad Enc(x)^{y_0}$ $\quad Enc(x)^{y_1}$

$\langle \varphi xy \rangle = DDL(Enc(x)^{\langle \varphi y \rangle})$ $\quad Enc(x)^{\varphi y_0}$ $\quad Enc(x)^{\varphi y_1}$

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

$(1 = z_1 \bmod N)$ $\quad z_0$ $\quad z_1$

$$\frac{Enc(x)^{y_1}}{Enc(x)^{y_0}} = Enc(x)^{y} = h^{ry}(1+N)^{2xy}$$

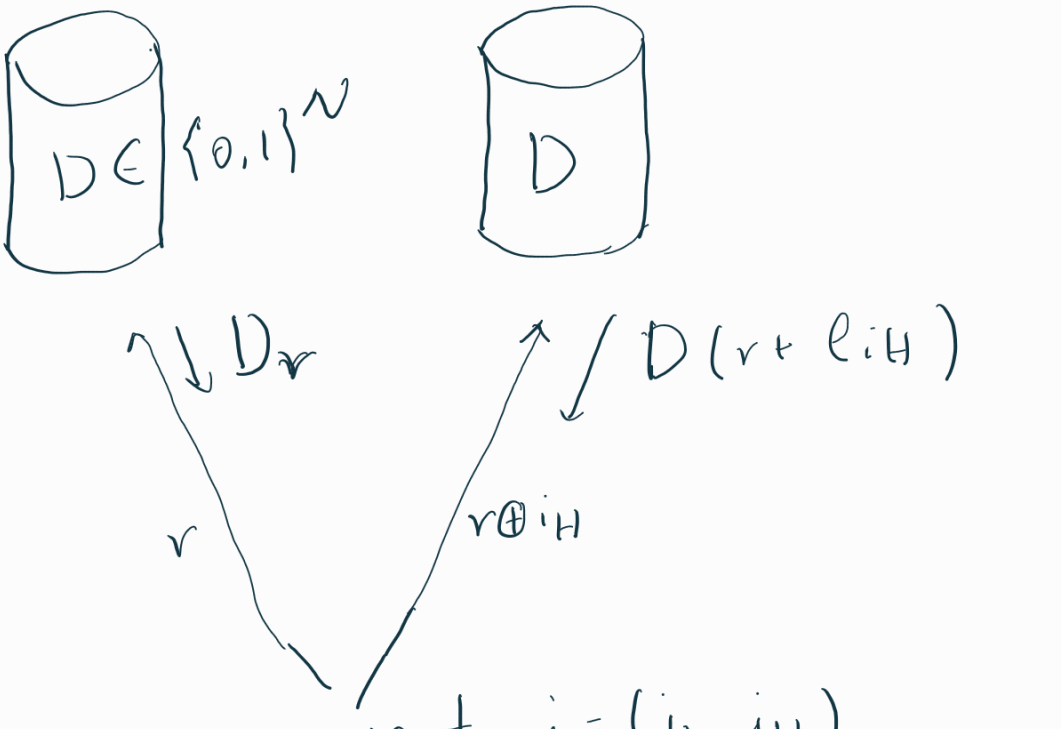
↓ 尝试令 $(p-1)(q-1) \mid ry$ 以消去 h^{ry}

$$\frac{Enc(x)^{\varphi y_1}}{Enc(x)^{\varphi y_0}} = (1+N)^{2\varphi xy}$$

Information-Theoretic Cryptography

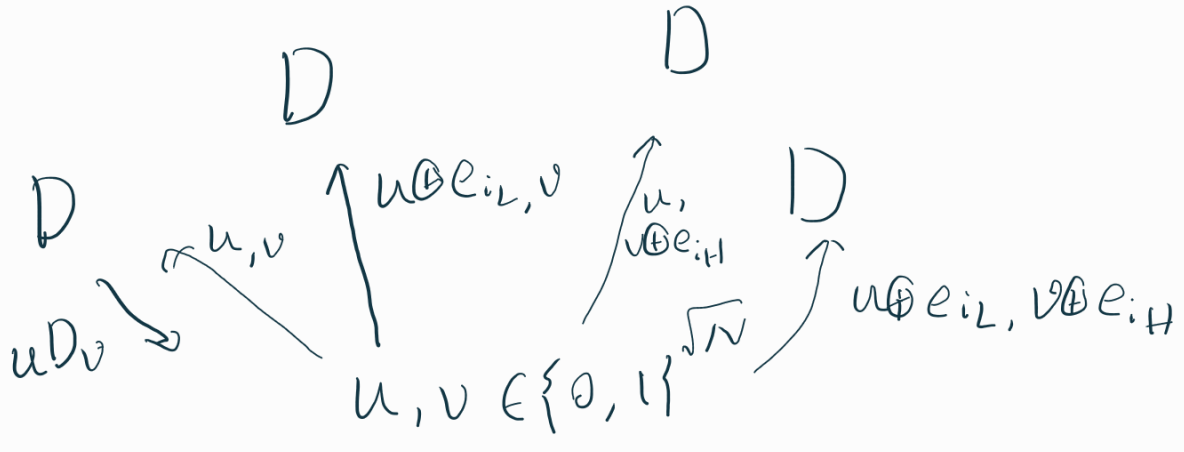
- Private Information Retrieval (PIR)
- Conditional Disclosure of Sends (CDS)
- Private, Simultanous Messages (PSM)
- Randomized Encoding
- Distributed Point Function

PIR



$D[i] = e_{i_L}^T D e_{i_H}$

if more servers:

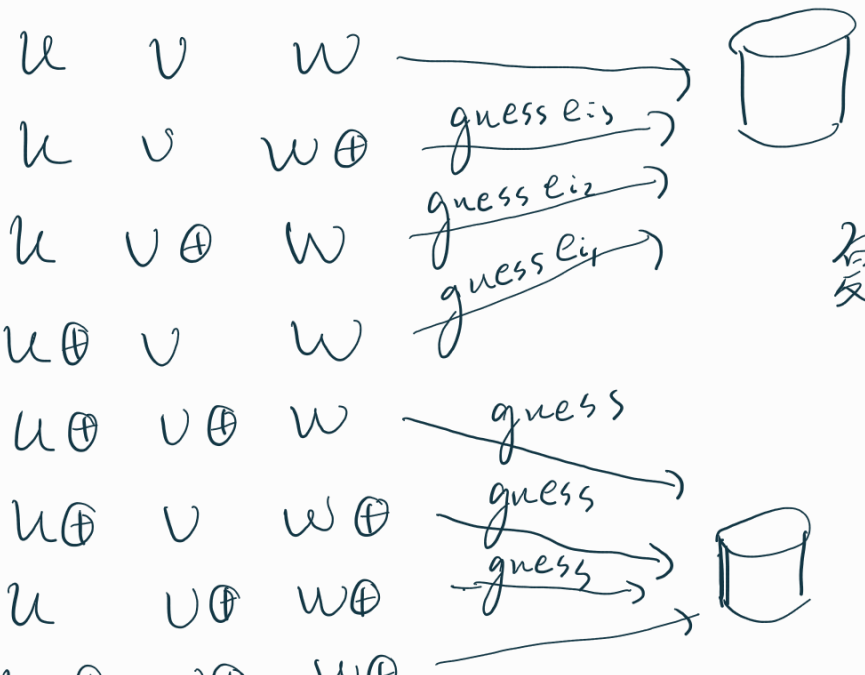


将四个返回值 xor，得 $e_{i_L} D e_{i_H}$

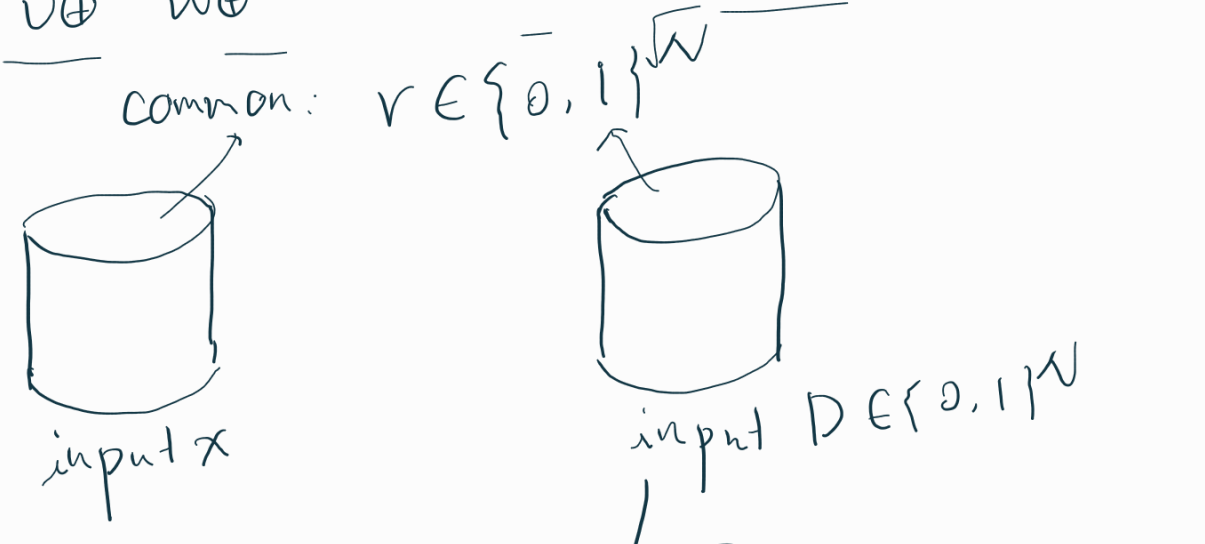
* if two servers

u, v, w

$e_{i_1}, e_{i_2}, e_{i_3}$



复杂度 $O(\sqrt[3]{N})$

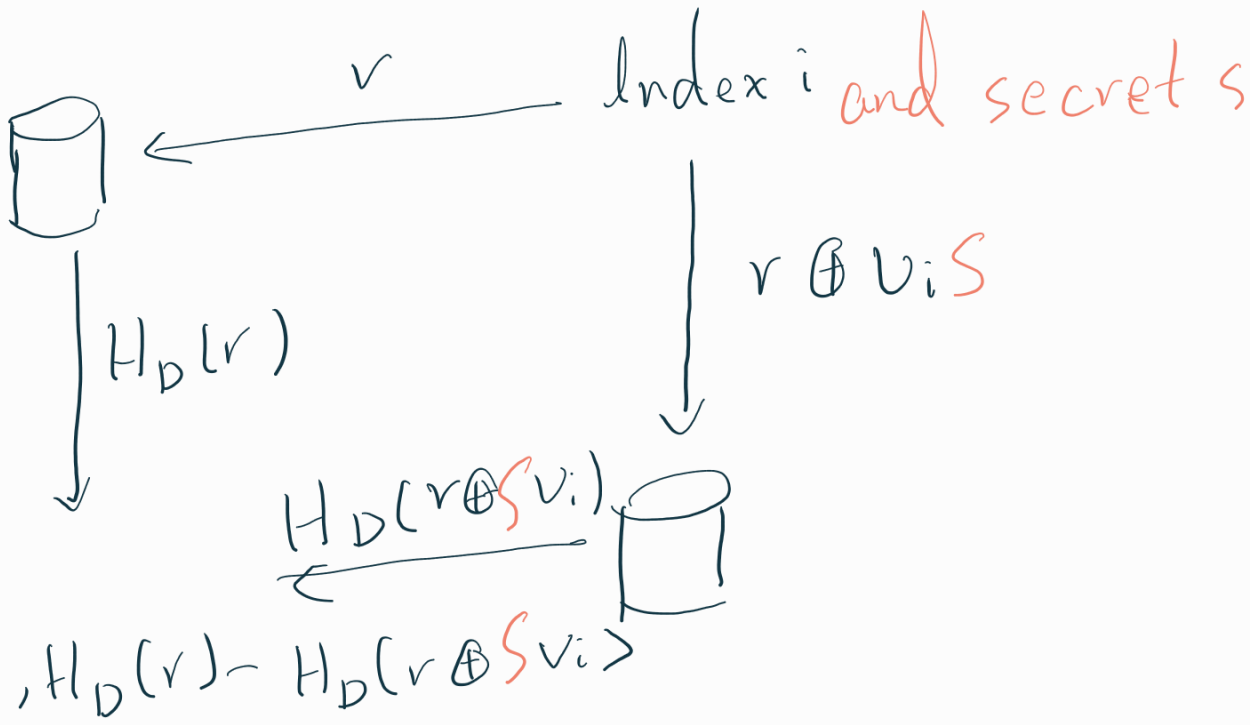


$e_{x_L} Dr$

$\oplus$

$e_{x_L} D(r + S \cdot e_{x_H}) = S\ D(x)$

PIR ⟶ CDS



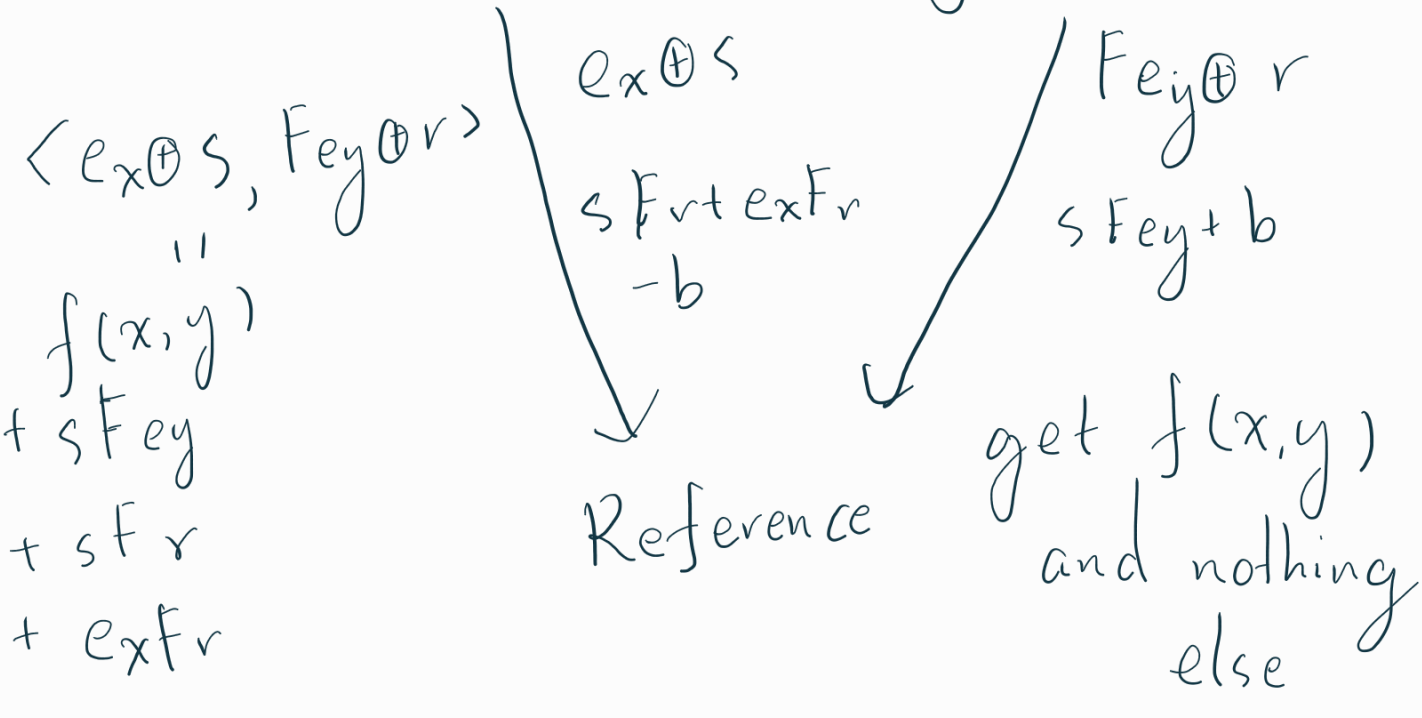
PSM

common random string

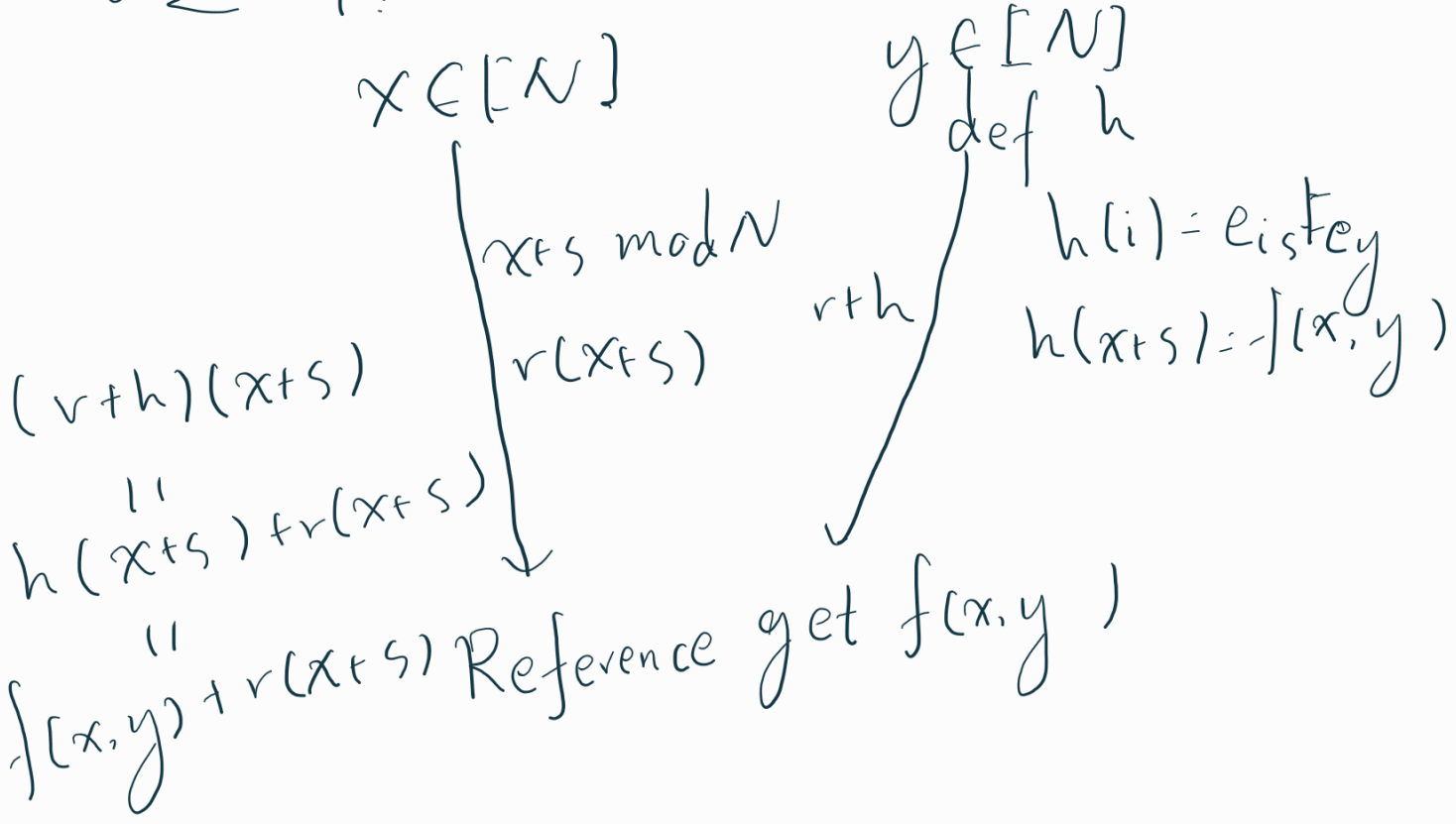
s, r, b

x ∈ [N]

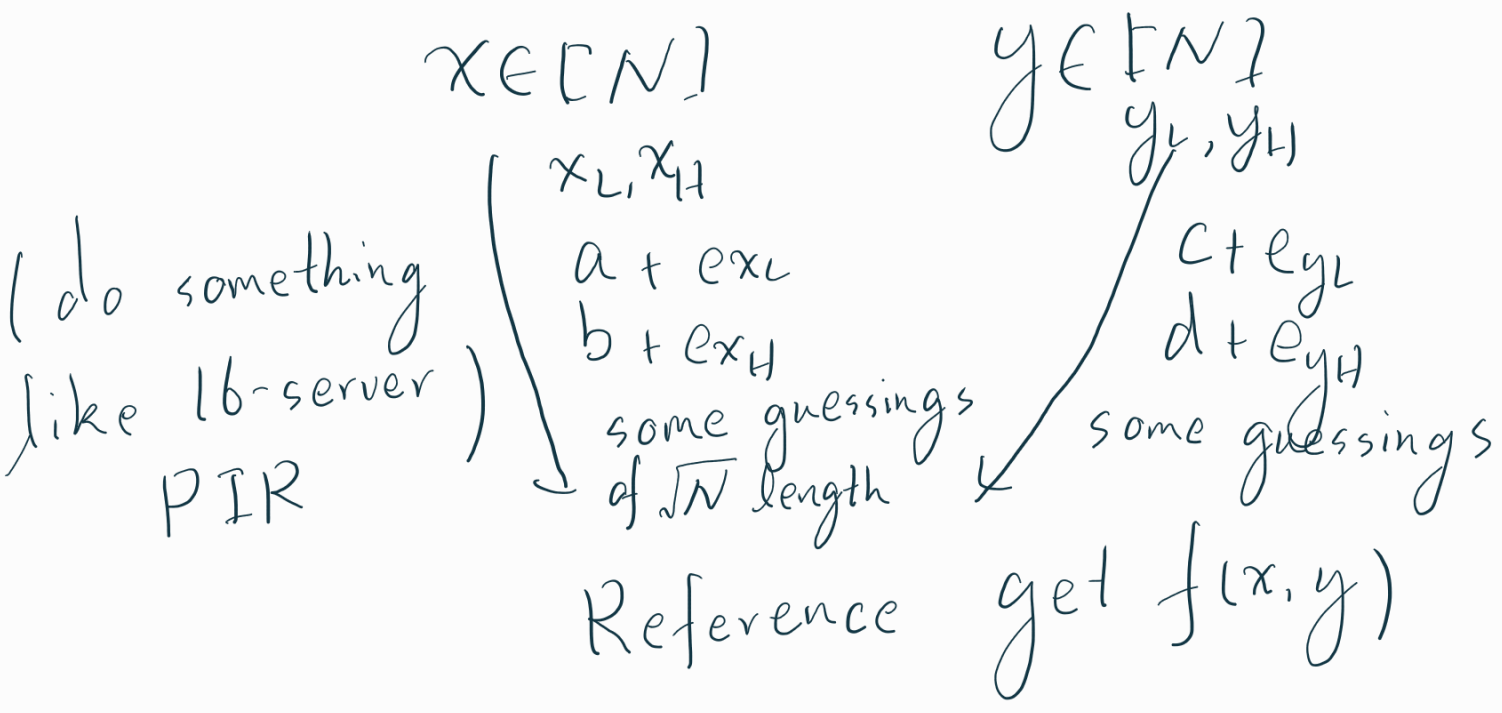
y ∈ [N]



改进一下：


x∈[N]
y∈[N]
def h
x+s mod N
r(x+s)
r+h
h(i) = e_i + e_y
h(x+s) = -f(x,y)
(r+h)(x+s)
=
h(x+s)+r(x+s)
=
f(x,y)+r(x+s)
Reference
get f(x,y)

再改进


x∈[N]
y∈[N]
y_L, y_H
x_L, x_H
a + e_xL
b + e_xH
some guessings
of √N length
c + e_yL
d + e_yH
some guessings
(do something
like 1b-server
PIR)
Reference
get f(x,y)