Homomorphic Secret Sharing (HSS)

Alice Bob

share(x) ⟶ x_0 x_1

↓ ↓

$f(x)$ ⟵ (Reconstruct) y_0 y_1

		ALICE		BOB
additive share	$\langle x \rangle$ =	$-x_0$	+	x_1
	$\langle y \rangle$ =	$-y_0$	+	y_1
	$\langle x+y \rangle$ =	$-(x_0+y_0)$	+	(x_1+y_1)

乘法？发挥是 ElGamel Encryption $Enc(k,x) = (h_1, h_2 = h_1^k g^x)$

其中 $pk = (g, g^k)$

给定 $\langle y \rangle$ y_0 y_1

计算 $h_2^{\langle y \rangle}$ $h_2^{y_0}$ $h_2^{y_1}$

这表明 $\frac{h_2^{y_1}}{h_2^{y_0}} = h_2^{y} = h_1^{ky} g^{xy}$

额外发送 $\langle ky \rangle$ $\overline{y_0}$ $\overline{y_1}$

计算 $h_2^{\langle y \rangle} / h_1^{\langle ky \rangle}$ $h_2^{y_0} \cdot h_1^{\overline{y_0}}$ $h_2^{y_1} \cdot h_1^{\overline{y_1}}$

则 $\frac{h_2^{y_1} h_1^{\overline{y_1}}}{h_2^{y_0} h_1^{\overline{y_0}}} = g^{xy}$

令 $z_0 = h_2^{y_0} h_1^{\overline{y_0}}$ $z_1 = h_2^{y_1} h_2^{\overline{y_1}}$，有 $z_1 / z_2 = g^{xy}$

即 $DL(z_0)$ $DL(z_1)$ 是 $\langle xy \rangle$ 的 addictive share

问题：不会计算 discrete log ⟹ 做 DDL

在循环群上找定若干点，希望：z_0 和 z_1 到达找定点步数的差是 xy

添加 assumption：Bounded integer B

令找定点差异：B·poly，则错误概率为 poly

用 PRF/Hash function 确定找定点

No.

Date. . .

$\langle xy \rangle = DDL(h_2^{\langle y \rangle} / h_1^{\langle ky \rangle})$

$\Rightarrow Enc(k, kx) = (T_1, T_2)$

$\langle kxy \rangle = DDL(T_2^{\langle y \rangle} / T_1^{\langle ky \rangle})$

Paillier encryption

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

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

或 $= r^N \cdot (1+N)^{2m}$

additive share $\langle x \rangle$ x_0 x_1

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

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

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

注意到 $h^{(p-1)(q-1)} = 1$

$\varphi := (p-1)(q-1)$

$\langle \varphi y \rangle$ $\overline{y_0}$ $\overline{y_1}$ $\left(\frac{Enc(x)^{\overline{y_1}}}{Enc(x)^{\overline{y_0}}} = Enc(x)^{\varphi y} = (1+N)^{2xy\varphi} \right)$

令 $z_0 = Enc(a)^{\overline{y_0}}$ $z_1 = Enc(x)^{\overline{y}} = z_0 (1+N)^{2xy\varphi}$

注意到 $\forall a \in \mathbb{Z}_{N^2}$, $a = (a \bmod N)(1+N)^{a'}$

$\therefore z_0 = r(1+N)^{z_0'}$ $z_1 = r(1+N)^{z_0' + 2xy\varphi}$

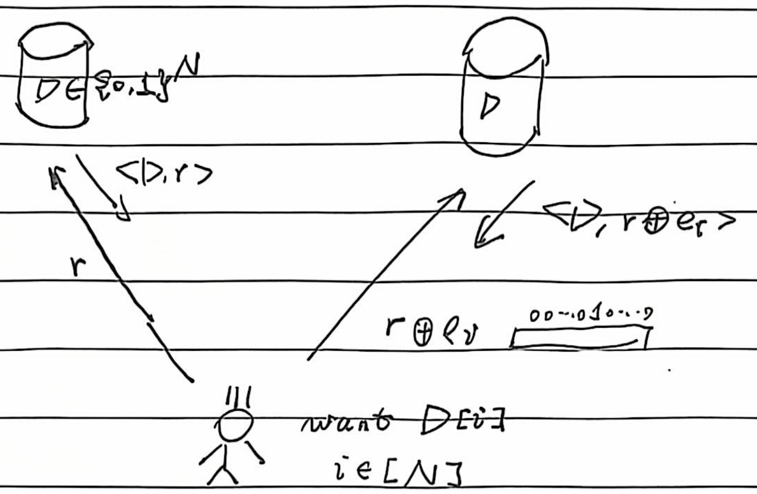
其中 $r = z_0 \bmod N = z_1 \bmod N$

得到 $\langle \varphi xy \rangle =$

需要把 N, N^2 变 N^b, N^{1+b} 以减少 domain 转换造成错误的概率

Information-Theoretic Cryptography

— Private Information Retrieval (PIR)



改进：

令 $\sqrt{N} \times \sqrt{N}$ D　　$i = (i_L, i_H)$　记作 $r \oplus e_{i_H}$

则 $D[i] = e_{i_L}^T D e_{i_H}$

更多 server：

$u, v \in \{0,1\}^{\sqrt{N}}$

分别发送 (u, v)　$(u \oplus e_{i_L}, v)$　$(u, v \oplus e_{i_H})$　$(u \oplus e_{i_L}, v \oplus e_{i_H})$

得到 uDv 和 $(u \oplus e_{i_L})Dv$ …

异或和为 $e_{i_L} D e_{i_H}$

进一步拆分 index：

$i = (i_1, i_2, i_3)$　需要 8 个 server

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

发送　u　v　w

　　$u \oplus e_{i_1}$　$v \oplus e_{i_2}$　$w \oplus e_{i_3}$

减少 server：

通信方面：收到 u, v, w，每次能为 1 的比特，将 $\sqrt[3]{N}$ 种情况全部发送

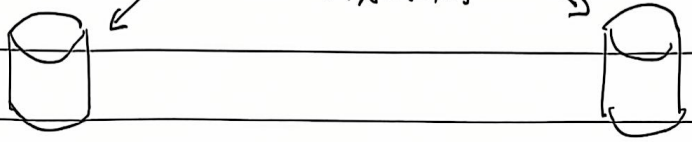
No.

Date. . .

— Conditional Disclosure of Secrets (CDS)

Common random string

$r_1, \dots, r_N \in \{0,1\}$



input of secret S

input y ($D \in \{0,1\}^N$)

$r_1, r_2, \dots, r_x \oplus s, \dots, r_N$

$\oplus_{D(i)=1} r_i$

gets S if $P(x,y)=1$ ($D(x)=1$)

input x, y (x, D)

balance :

D $r \in \{0,1\}^m$ $x = (x_1, x_N)$

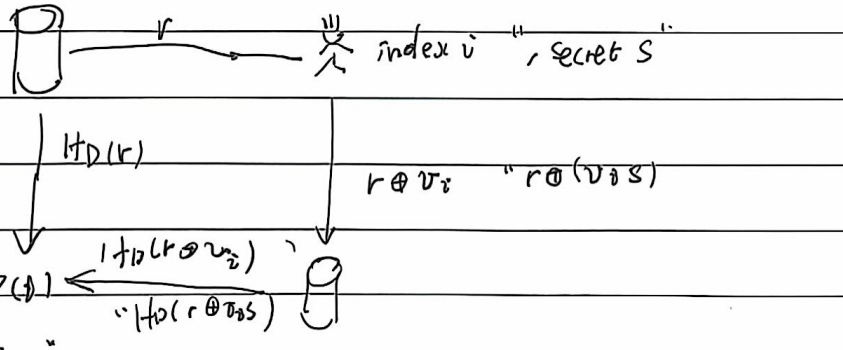
left : $r + s \cdot e_{x_H}$ right : Dr

对 client 得到 $e_{x_L}(Dr)$ 和 $e_{x_L} D(r + s e_{x_H})$

并线得 $S \cdot D(x)$

secure : left $r + s \cdot e_{x_H} + e_{x_L}^T \cdot w$ right $Dr + w$

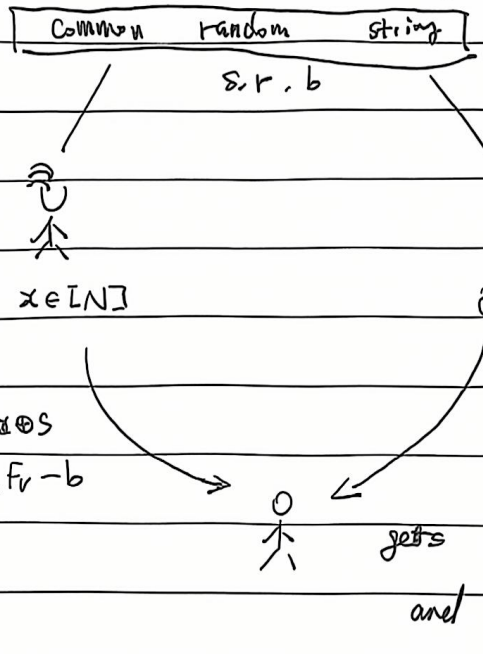
PIR → CDS :



No.

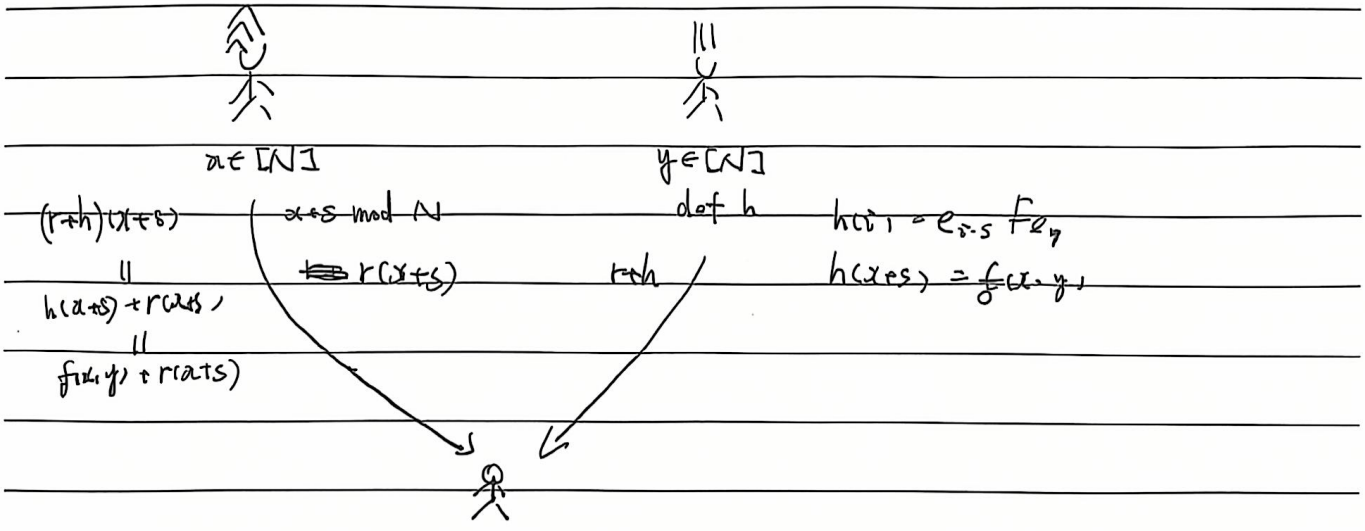
Date. . .

- Private Simultaneous Messages (PSM)



$N \boxed{f} N$ $\quad f(x,y) = e_x F e_y$

$\langle e_x \oplus s,\ F e_y \oplus r \rangle = f(x,y) + sF e_y + sF_r + e_x F_r$



证明：$f(x_1, x_{11}, y_1, y_{11})$ multilinear 下

$= F(e_{x_1}, e_{x_{11}}, e_{y_1}, e_{y_{11}})$

No.

Date. . .

left: $a+e_{x_1}$ right: $c+e_{y_1}$

$b+e_{x_1+1}$ $d+e_{y_1+1}$

$F(a+e_{x_1}, \dots) = F(a,b,c,d) + \dots$

考法 $F(e_{x_1}, e_{x_1+1}, e_{y_1}, d) = F_{x,d}(e_{y_1})$ (linear-function)

$\Leftrightarrow \sqrt{N}$

2 PTR $\text{polylog}(N) \overset{\text{c.c.}}{\subseteq} 2^{\sqrt{\lg N \lg\lg N}}$

cDS $\Omega(\lg N) \subseteq \text{c.c.} \subseteq 2^{\sqrt{\lg N \lg\lg N}}$

PSM $3\lg N \subseteq \text{c.c.} \subseteq \sqrt{N}$

- Randomized Forwarding
- Distributed Point Function