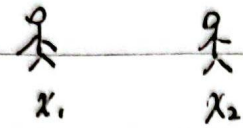
Date.

2PC 2-party computation

e.g. 百万富翁问题



$f(x_1, x_2) = (y_1, y_2)$

▷ Oblivious Transfer (不经意传输) (OT)

Sender  Receiver 

m_0, m_1 ← input → $b \in \{0,1\}$

ϕ ← output → m_b

(random oblivious transfer ver.

$b \xleftarrow{\$} \{0,1\}$

receiver gets (b, m_b))

▷ Trapdoor OWP → OT

semi-honest ⇒ computational secure

Sender

F, trapdoor

random Δ

$\xrightarrow{F, \Delta}$

$\xleftarrow{y_0, y_1 \ (y_0 + y_1 = \Delta)}$

Receiver

$y_b := F(x_b)$ $x_b \xleftarrow{\$} \dots$

$y_{1-b} := \Delta - y_b$

$x_0 := F^{-1}(y_0)$

$x_1 := F^{-1}(y_1)$

$\xrightarrow{HCB(x_0) \oplus m_0 \quad HCB(x_1) \oplus m_1}$

use x_b → m_b

semi-honest ⇒ perfect secure

▷ homomorphic encryption → OT

$\xleftarrow{Enc(b)}$

$\xleftarrow{Enc(m_0)}$

$(m_1 - m_0)\, Enc(b) + m_0 = Enc(m_b)$

$\xrightarrow{}$

maybe refresh?

No.

Date . . .

▷ Oblivious Linear Function Evaluation (OLE)

	Sender	Receiver
input :	$a, b \in \mathbb{F}$	$x \in \mathbb{F}$
output :		$ax+b$

▷ Palliar + public parameter → OLE

public :

pp : N^2, g, h ($N=1$ ~~$N+1$~~) ← hard group generators

Sender (a, b)		Receiver (x)
	$c := g^s h^{-r}$	$s, s', r \xleftarrow{\$} \dots$
	$c' := g^{s'} h^{-x+r}$ ←	
$t, w \xleftarrow{\$} \dots$		
	g^t	
$Enc(a) := h^t (N+1)^a$		$Enc(a)^x \cdot Enc(w) \cdot Enc(b-w)$
$Enc(w) := c^t (N+1)^w$		$= \dots$
$Enc(b-w) := c'^t (N+1)^{b-w}$	→	$= (N+1)^{ax+b} g^{t(s+s')}$
	use g^t log	$ax+b$.

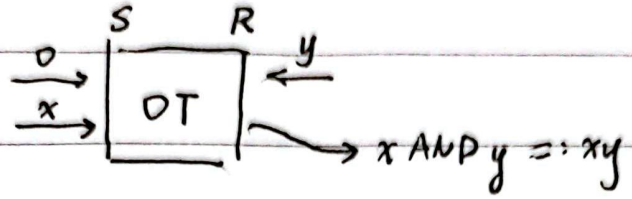
- malicious sender: get nothing about x. Simulator works with sk
- malicious receiver: let $h' := (1+N)h$ ($Enc(1) \approx Enc(0)$)

No.

Date . . .

AND with OT

x AND y :



~~Secret Sharing~~ Goldreich-Micali-Wigderson (GMW) protocol.

Alice	Bob	$[x]$
x_A	x_B	$[x]$
y_A	y_B	$[y]$
$x_A \oplus y_A$	$x_B \oplus y_B$	$[x \oplus y]$
?	?	$[xy]$ ← $xy = (x_A \oplus x_B)(y_A \oplus y_B) = \cdots$
$x_A y_A$	0	$[x_A y_A]$ ⊕
$\{0,1\} \xrightarrow{\$} r$	$x_A y_B \oplus r$	$[x_A y_B]$ ⊕
...	...	$[x_B y_A]$ ⊕
		$[x_B y_B]$

S R
→ →
OT

(generalize to n-party).

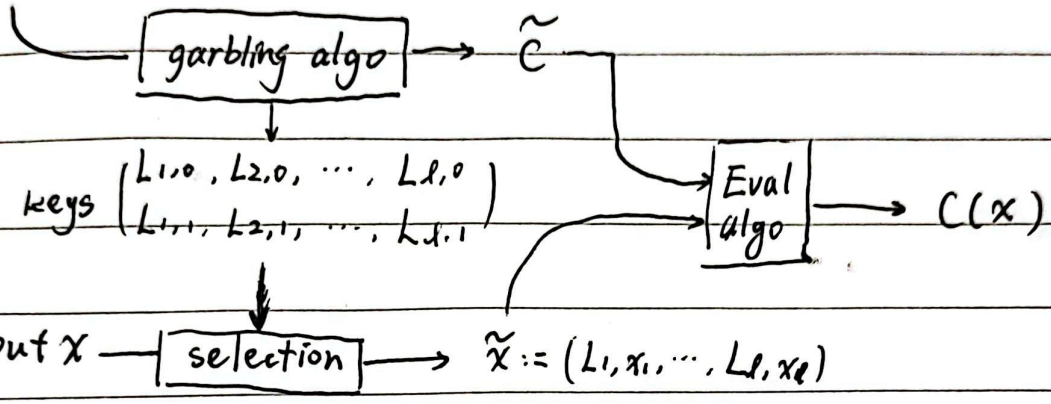
too many messages => too slow

No.

Date. . .

▷ Yao's Garbled Circuit. (混淆电路)

$C : \{0,1\}^l \to \{0,1\}^m$.

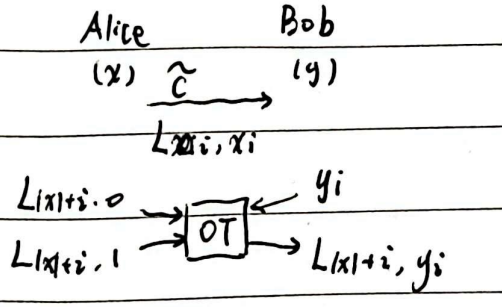


i) Correctness : $Eval(\tilde{C}, \tilde{x}) = C(x)$

ii) Security :

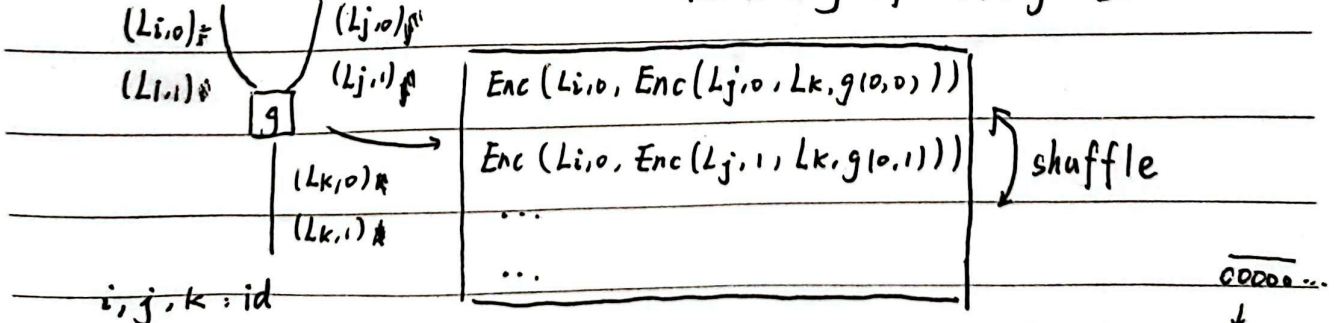
$\exists$ p.p.t Simulator S. s.t. $Sim(C, C(x)) \approx_c (\tilde{C}, \tilde{x})$

▷ Apply on 2PC :



▷ construction goal : Learn $L_k, g(x,y)$

Get nothing of $L_{k,1-g(x,y)}$



e.g. $F(L_{i,0}, k) \oplus F(L_{j,0}, k) \oplus (L_{k,g(0,0)} \cdots\cdots)$

F is PRF

No.

Date. . .

▷ color bit permute bit : α_i , real value : x_i

color bit : $\alpha_i \oplus x_i =: \tilde{x}_i$ ⟶ public

then shuffle the table by (α_i, α_j).

use $(\tilde{x}_i, \tilde{x}_j)$ to get ⟵

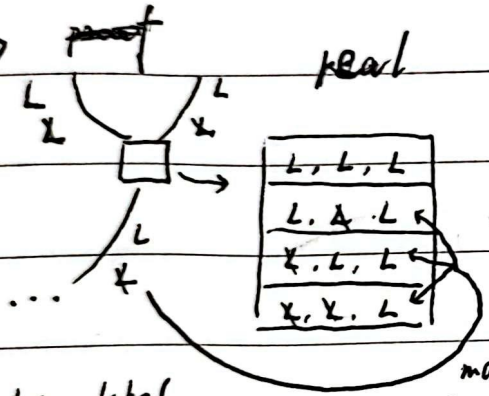
$(0,0) \to (\alpha_i, \alpha_j)$

$(0,1) \to (\alpha_i, 1 \oplus \alpha_j)$

$(1,0) \to \dots$

$(1,1) \to \dots$

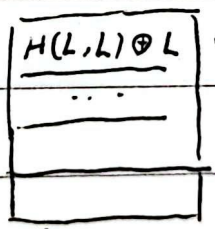
▷ proof



L : label

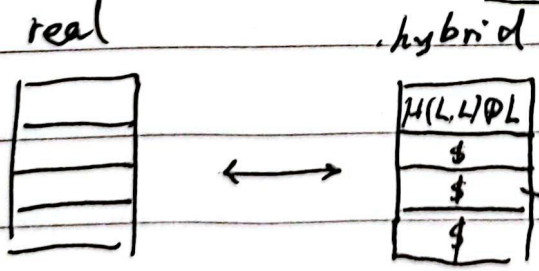
L : hidden label

another proof : table :



$H(L_{i,0}, L_{j,0}, k) \oplus L_{k,g[0,0]}$

....



use RO

let $H(\tilde{x}, L) = \dots$