2PC

2-party computation

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

Oblivious Transfer $\Longleftrightarrow$ Random Oblivious Transfer

	Sender	Receiver
input	$m_0 \quad m_1$	$b \in \{0,1\}$
output		m_b

Random Oblivious Transfer

input m_0, m_1

output $\qquad b \xleftarrow{\$} \{0,1\}, m_b$

Trapdoor OWP $\to$ OT

Sender $\qquad\qquad$ Receiver

F, trapdoor

random Δ $\quad \xrightarrow{F,\ \Delta}$ $\quad$ sample $y_b = F(x_b)$

$\xleftarrow{y_0, y_1,\ s.t\ y_0 + y_1 = \Delta}$

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

$x_1 = F^{-1}(y_1)$ $\quad \xrightarrow{HCB(x_0) \oplus m_0,\ HCB(x_1) \oplus m_1}$

Semi-honest Receiver: computational secure

Semi-honest Sender: Perfect secure

Sender $\qquad\qquad$ Receiver

$\xleftarrow{Enc(b)}$

$(m_1 - m_0) \cdot Enc(b) + m_0$

$\|$

$\xrightarrow{Enc(m_b)}$

Oblivious Linear Function Evaluation (OLE)

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

Palliar + public parameter $\longrightarrow$ OLE $\qquad$ p.p.: $N^2, g, \overset{\text{hard group}}{h}$

Sender $\qquad\qquad$ Receiver

a, b $\qquad \xleftarrow{Enc(x)}$ $\qquad x$

$\xrightarrow[Enc(ax+b)]{}$

Sender a, b Receiver x, $s, s', r \xleftarrow{\$}$

$$\underbrace{g^s h^{-r}}_{C}, \underbrace{g^{s'} h^{-x+r}}_{C'} \quad \longleftarrow$$

$t \xleftarrow{\$}$

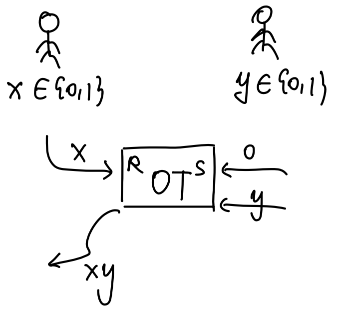
$$g^t \cdot \big(\overbrace{h^t (N+1)}^{Enc(a)}\big)^a \longrightarrow$$

$$\underbrace{C^t (N+1)^w}_{Enc(w)}, \underbrace{(C')^t (N+1)^{b-w}}_{Enc(b-w)}$$

$$h^{xt} (N+1)^{ax} \cdot (g^s h^{-r})^t \cdot (N+1)^w \cdot (g^{s'} h^{-x+r})^t \cdot (N+1)^{b-w}$$

$$= (N+1)^{ax+b} \cdot g^{t(s+s')}$$

Simulator: generate Protocol



x	y		
x_A	x_B	$[x]$	
y_A	y_B	$[y]$	
$x_A \oplus y_A$	$x_B \oplus y_B$	$[x \oplus y]$	
z_A	z_B	$[xy]$	
$x_A y_A$	0	$[x_A y_A]$	$z_A \oplus z_B = xy$
0	$x_B y_B$	$[x_B y_B]$	
r	$\boxed{OT} \to x_A y_B \oplus r$	$[x_A y_B]$	$= (x_A \oplus x_B)(y_A \oplus y_B)$
	same as $x_A y_B$	$[x_B y_A]$	$= x_A y_A \oplus x_A y_B \oplus x_B y_A \oplus x_B y_B$

Multi-Party (GMW Goldreich-Micdi-Wigderson)

				additive share
x_1	x_2	x_3	x_4	$[x]$ s.t. $\sum x_i = x$
y_1	y_2	y_3	y_4	$[y]$
$x_1 + y_1$	. . . .		$x_4 + y_4$	$[x+y]$
				$[xy]$
r	$x_1 y_2 - r$	0	0	$[x_1 y_2]$

Yao's Garbled Circuit

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

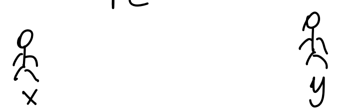
garbling algo $(C) \longrightarrow \tilde{C}$

n keys $\begin{pmatrix} L_{1,0} & L_{2,0} & L_{3,0} & \cdots & L_{\ell,0} \\ L_{1,1} & L_{2,1} & L_{3,0} & \cdots & L_{\ell,1} \end{pmatrix}$

input $x \in \{0,1\}^\ell \xrightarrow{\text{selection}} \underbrace{L_{1,x_1},\ L_{2,x_2} \cdots}_{\text{labels}}$

$\boxed{\text{Evaluation algo}} \to C(X)$

2PC



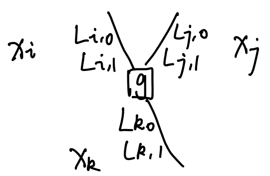
$\tilde{C}$
$\xrightarrow[L_{1,x_1},\ L_{2,x_2} \cdots]{}$

$L_{|x|+i,0}$, $L_{|x|+i,1} \rightrightarrows \boxed{OT} \leftarrow y_i$

$\boxed{OT} \to L_{|x|+i,y_i}$

Security: $\tilde{C}$, $(L_{i,x_i})_i$ leaks no more than C, $C(X)$

$\tilde{C}, (L_{i,x_i})_i \approx_c Sim(C, C(X))$



wish that:
given $L_{i,x}$ $L_{j,y}$
$L_{k,g(x,y)}$ is revealed
$L_{k,1-g(x,y)}$ is hidden

x: real value
permute bit $\to \alpha_i$
color bit $\to x \oplus \alpha_i$
$lsb(L_{i,b}) = b \oplus \alpha_i$

PRF

Table

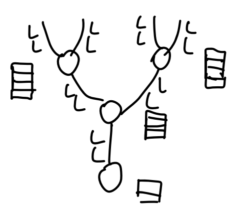
$F(L_{i,0}, k)$ ⊕	$F(L_{j,0}, k)$ ⊕	$L_{k,g(0,0)}$
0	1	01
1	0	10
1	1	11

shuffle $\alpha_i \alpha_j$

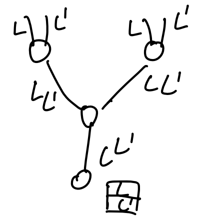
0, 0	α_i	α_j
0, 1	α_i	$1 \oplus \alpha_j$
1, 0	$1 \oplus \alpha_i$	α_j
1, 1	$1 \oplus \alpha_i$	$1 \oplus \alpha_j$

$F(L_{k,0}, k \| \cdots)$
$F(L_{k,1}, k \| \cdots)$

real world



simulation



$E(L, E(L, L'))$
$E(L, E(L', 0))$
$E(L', 0)$
$E(L', 0)$

Mult- Party

Approach I

P_i sample $L_{j,b}^{(i)}$

def $L_{j,b} = \bigoplus_i L_{j,b}^{(i)}$

Approach II

P_i samples $L_{j,b}^{(i)}$

def $L_{j,b} = L_{j,b}^{(1)} \| L_{j,b}^{(2)} \| L_{j,b}^{(3)} \| \cdots$