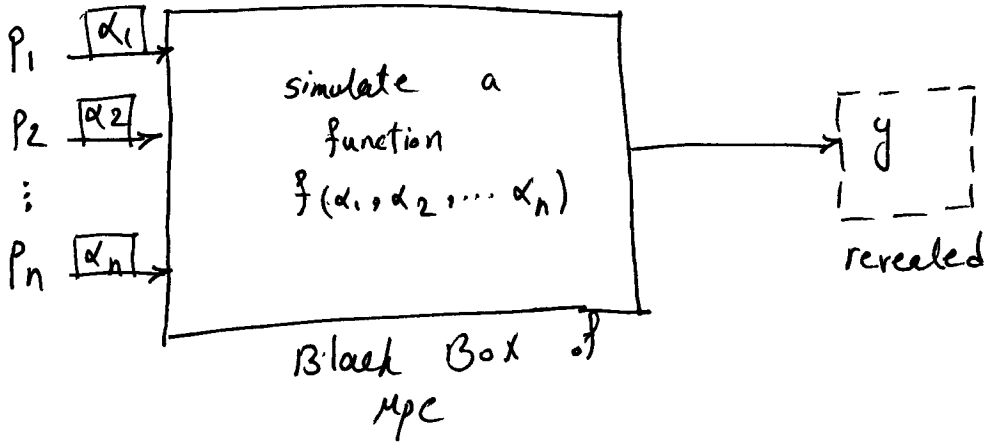
lec 10

Secure Multiparty Computation (MPC)

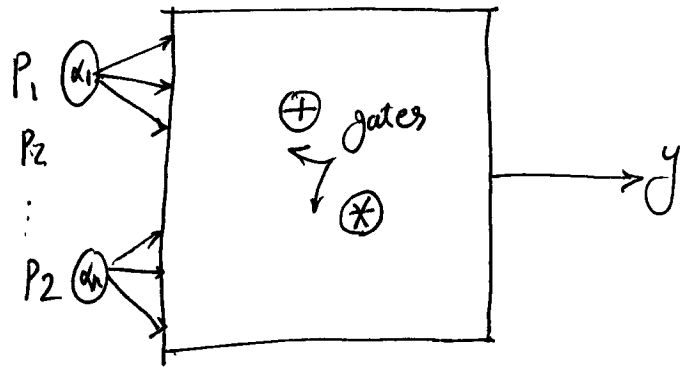
we have n players $P_1 \cdots P_n$ where each party holds a private value. The goal is to calculate a function over these private values without revealing these values. At the end of computation, only the function value will be revealed to every one.



① Arithmatic Cir ⟶ field elemets ⟶ $\oplus$ $\circledast$

② Boolean Cir ⟶ single Bit ⟶ $\wedge$ $\vee$, ...

⟶ secret sharing



Applications

① Sealed-Bid Auctions

↳ to protect the losing bids for future auctions

② Secure set interseection problem

↳ only reveal common names from 2 lists

(a) **Equality check**

$\alpha_1 \longrightarrow$ shared secret among n players

$\alpha_2 \longrightarrow$

$\gamma * (\alpha_1 - \alpha_2) = \begin{cases} 0 \rightarrow \text{equal} \\ \neq 0 \rightarrow \text{not equal} \end{cases}$

γ: random secret $\neq 0$

we use γ to prevent revealing the difference between two secrets α_1 & α_2

(b) **Comparison:** to show which secret is smaller or larger.

(a) & (b) → list of elements → we can (c) **find Max or Min** element in a secret list

↳ using Equality check, Comparison, Min & Max operations, we can (d) **Sort** a list of secret values without revealing those values

* too many other operation & computations can be executed by MPC

$f_1(x) = \alpha_1 + a_1 x + a_2 x^2 + \cdots \longrightarrow f_1(1)\ f_1(2)\ \ldots\ f_1(n)$ (P1 P2 ... Pn)

$f_2(x) = \alpha_2 + b_1 x + b_2 x^2 + \cdots \longrightarrow f_2(1)\ f_2(2)\ \ldots\ f_2(n)$

$f_1(1) + f_2(1)\quad f_1(2) + f_2(2) \ldots$ ⊕

LI ← $f_1(x) + f_2(x)$ ← $f_1(1) * f_2(1)\quad f_1(2) * f_2(2) \ldots$ ⊛

$\alpha_1 + \alpha_2$ ← new secret; $f_1(x) + f_2(x)$ ← new secret sharing poly

degree remains the same

$\alpha_1 * \alpha_2$ ← $f_1(x) * f_2(x)$

* degree will be increased

threshold $t=3$

$f(x) = 3 + x + x^2$

$g(x) = 2 + x + x^2$

$\mathbb{Z}_p \longrightarrow p = 41$

	P_1	P_2	P_3	P_4	P_5
shares on $f(x)$ →	5	9	15	23	33
shares on $g(x)$ →	4	8	14	22	32
shares on $f(x)+g(x)$ ⊕	9	17	29	4	24
shares on $f(x)*g(x)$ ⊛	20	31	5	14	31

$f+g = 5 + 2x + 2x^2$ → new secret

$f*g$ → new

$f*g = 6 + 5x + 6x^2 + 2x^3 + x^4$ → $t = 5$ new threshold

$H(x) = 6 + h_1 x + h_2 x^2$

Degree reduction in MPC

publicly known

$$\begin{bmatrix} \text{VDM} \end{bmatrix} \begin{bmatrix} \text{coeff} \end{bmatrix} = \begin{bmatrix} \text{eval} \end{bmatrix}$$

$f(x)$ — eval on $f(x)$

$$\begin{matrix} x=1 \\ x=2 \\ x=3 \\ \vdots \end{matrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 2^2 \\ 1 & 3 & 3^2 \\ \vdots & \vdots & \vdots \end{bmatrix} \begin{bmatrix} 3 \\ 1 \\ 1 \\ \vdots \end{bmatrix} = \begin{bmatrix} 5 \\ 9 \\ 15 \\ \vdots \end{bmatrix} \longrightarrow \begin{bmatrix} \text{VDM} \end{bmatrix} \begin{bmatrix} \text{coeff} \\ \text{of } H(x) \end{bmatrix} = \begin{bmatrix} \text{eval} \\ \text{of } 0 \end{bmatrix} = \begin{bmatrix} 0 \end{bmatrix}$$

$$\begin{bmatrix} 6 \\ 5 \\ 6 \\ 2 \\ 1 \end{bmatrix} = \underbrace{\begin{bmatrix} 5 & 31 & 10 & 36 & 1 \\ 38 & 11 & 1 & 17 & 15 \\ 32 & 38 & 2 & 0 & 10 \\ 37 & 9 & 38 & 36 & 3 \\ 12 & 34 & 31 & 34 & 2 \end{bmatrix}}_{VDM^{-1}} \underbrace{\begin{bmatrix} 20 \\ 31 \\ 5 \\ 14 \\ 31 \end{bmatrix}}_{eval}$$

$q_1 * q_2$

$5*20 + 31*31 + 10*5 + 36*14 + 1*31 = 6$ ✓

f*g

re-sharing

P_1: $h_1(x) = 20 + x + x^2 \longrightarrow$ $[h_1(1) \quad h_1(2) \quad h_1(3) \quad h_1(4) \quad h_1(5)]$

$h_2(x) = 31 + x + x^2 \longrightarrow$ $[h_2(1) \quad h_2(2) \quad \cdots]$

$h_3(x) = 5 + x + x^2 \longrightarrow$

$h_4(x) = 14 + x + x^2 \longrightarrow$

P_5: $h_5(x) = 31 + x + x^2 \longrightarrow$

since we want to reduce the degree of f*g from 4 to 2, the re-sharing polys should have degrees of 2

$$P_1 \begin{bmatrix} h_1(1) \\ h_2(1) \\ h_3(1) \\ h_4(1) \\ h_5(1) \end{bmatrix} \underbrace{\begin{bmatrix} 5 & 31 & 10 & 36 & 1 \end{bmatrix}}_{VDM^{-1}}$$

$h_1(1)*5 + h_2(1)*31 + \cdots = H(1)$ single value is share of secret which is 6

on a new poly of degree 2

$H(x)$