Multi-Party Computation.

P_1 P_2 P_3 P_4 P_5.

x_1 x_2 x_3 x_4 x_5. input.

want: $(y_1, y_2, y_3, y_4, y_5) = f(x_1 \cdots x_5)$

↑ public.

定义 Protocol:

每一轮产生: $view_i^r \to m_{i\to j}^r$.

根据每一轮的 $f_i^r(view_i^r, m_{\cdot\to i}^r) \to view_i^{r+1}$

Correctness 都输出 $f(x_1 \cdots x_5)$.

Security.

weakest: Semi-Honest / Honest-but-curious.

~~存在 Sim_i, $Sim_i(x_i, y_i) \approx_{p/s/c} View_i^r$.~~

$\Rightarrow \exists S \subseteq [n]$, $View_S^r \approx Sim_S(x_S, y_S)$.

$\Rightarrow \forall S \subseteq [n], |S| \leq \text{threshold}$.

$View_S^r \approx Sim_S(x_S, y_S)$.

Secret Sharing.

Secret $S \xrightarrow{\text{algo}} (S_1, S_2, S_3, S_4, S_5)$.

1. Correctness. $\forall T, |T| > t$, $Recover(S_T) \to S$.
2. Security: $\forall T, |T| \leq t$, $(S_T) \equiv Sim(T)$.

设 $S \in$ Domain $\mathbb{F}$.

sample a polynomial f, s.t. $f(0) = S$, $deg = t$.

且 $f(i) = S_i$.

BGW Protocol.

eg. Want $\sum x_i$.

每个 Agent i 把自己的 Secret Sharing 发给所有

对 Agent i，仅需求和就会得到 $\sum x_i$ 的

Secret Sharing.

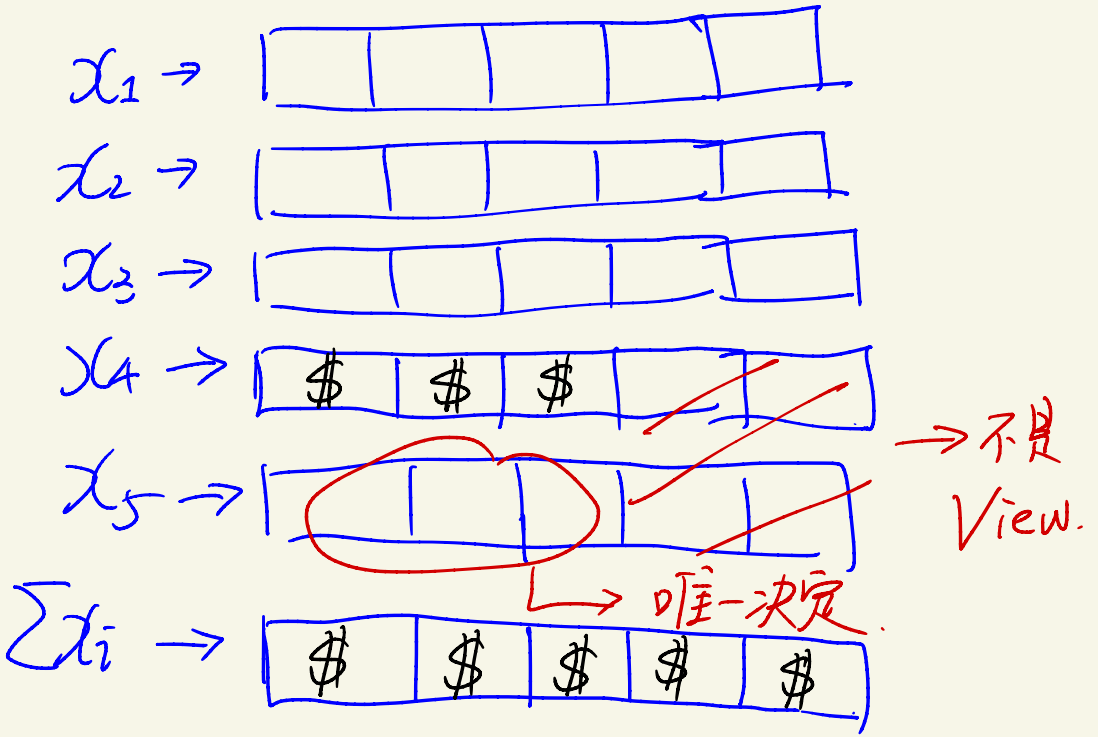
① Broadcast my secret Sharing.

*在 Secret Sharing 中选择 $t = n-1$.

denote as $[\sum x_i]_{n-1}$.

这是安全的. 如何构造 Sim?

Take $S = \{1,2,3\}$ as example.



由于 x_5 随机性. 这个是随机的.

计算 $x_1 x_2$

还是 Sharing $[x_i]_t$.

本地进行乘法. 也即 t 至多也只能 $n > 2t$. 不好.

需要 $[x_1 x_2]_{2t} \to [x_1 x_2]_t$.

refresh: 由于 Lagrange 插值是线性操作.

将我们刚刚的 $[x_1 x_2]_{2t}$ 作为一个计算 component.

$f(\cdots) = c_1 [x_1 x_2]^1_{2t} + c_2 [x_1 x_2]^2_{2t} \cdots\cdots$

用之前的办法 Protocol.

open: 有可能泄漏额外信息.

方法2: $[y] = c_1 y_1 + c_2 y_2 + \cdots + c_n y_n$.

和之前计算线性函数一样.

方法3: 生成 n 个 $[0]_{n-1}$, 求和得到一个

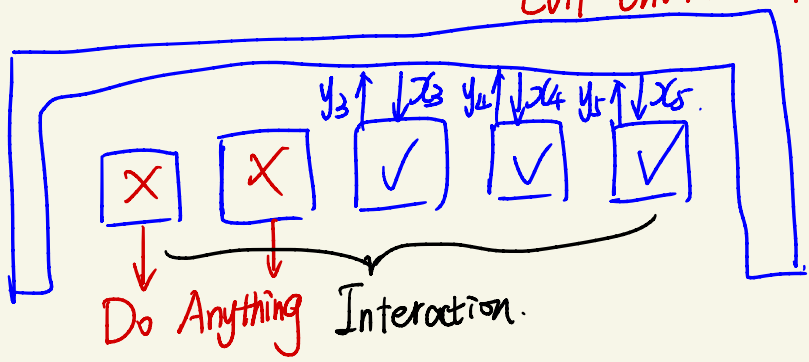
安全的 $[0]$ 的 Secret Sharing.

将 $[0]$ 加到自己序号输出上面即可.

$\Rightarrow$ BGW Protocol. Perfect Semi-honest tolerating $\frac{n-1}{2}$ corruption.

Malicious Attackers.

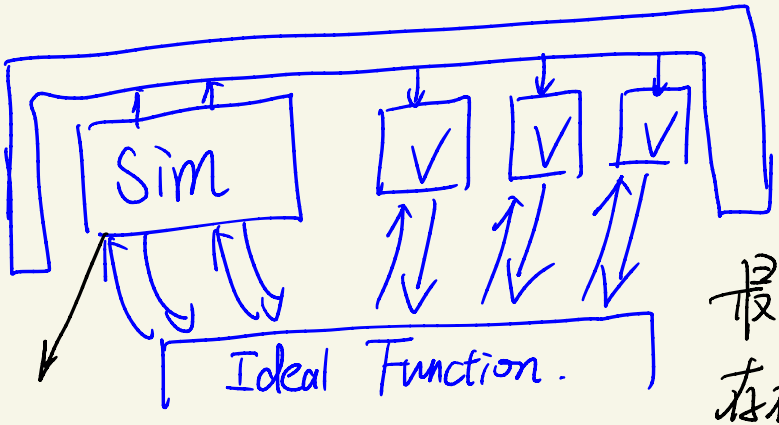
Evil Environment.



最理想的安全性.

Evil Party 可根据收入等消息发消息.

存在一个 Sim 如下:



Here
No Interaction.

最理想的情况:
存在一个第三方
帮你计算.

Environment 在两种情况下 View 不可区分.

Broadcast.

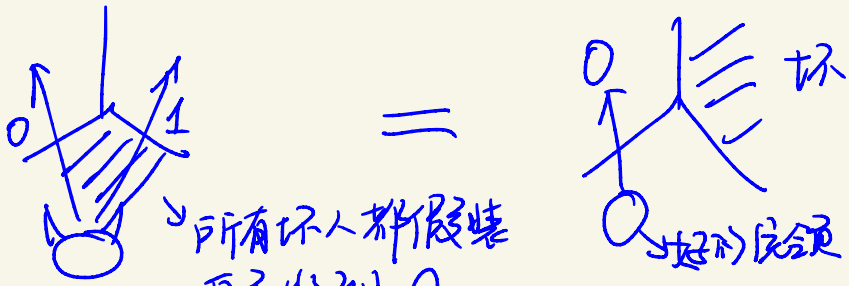
$f(x, \perp, \perp, \perp, \perp) = (x, x, x, x, x)$.

Byzantium Generals' Problem

① 若第一个 Party 是好的，所有输出都要等于 x.

② 若第一个 Party 不好，所有好人都要输出相同.

有 $\frac{1}{3}$ 的坏人，该问题无法解决.



亦似同理. 故 $\frac{1}{3}$ 以上无法解决.

Broadcast Problem with $t < 0.01n$.

verifiable SS.

sharing ($S \in \mathbb{F}$):

sample poly P, $\deg(p) \le (t, t)$.

s.t. $P(0,0) = S$.

$share_i = (p(i, \cdot), p(\cdot, i))$.

P_i, P_j 可以做一些检验如 $P(i,j)$ $P(j,i)$ 是否矛盾.
(若 j 是坏人, 即使无矛盾也可报告有矛盾).

现在 Distributor 分发一个 $p(i,j)$.
每个 Agent i, 广播 (i,j) 是否有矛盾. 无矛盾之间连边. 若存在一个 $n-t$ 的 clique, 则 Distributor 可以是好的.

然后每个人 i 问问其它人 $P(i,j)$ 是多少.
由于好人是好多, 已经能 Recover 多项式.

ZKP

P_1 P_2 P_3.

x_1, r_1

$H(x_1, r_1)$ ⟶ .

$(x_1, r_1, m^1_{i\to 1}, \pi^1_{i\to 1})$ $\xrightarrow{m^2_{1\to 2},\ \pi^2_{1\to 2}}$

Proof.

缺陷: 最后一轮
t 个人拿到消息跑路了.

Security w/ abort.

Semi-Malicious. (可以自行选择 random bits)

↓ ZKP.

Security w/ selective Abort.

↓ Broadcast.

Security w/ Abort.

Randomized Encoding (RE).

$\hat{f}$ is an RE of f

1) $f(x)$ is equivalent with $\hat{f}(x,r)$.

2) $\hat{f}$ is simple.

1.1). $\exists$ p.p.t. Dec

$$Dec(\hat{f}(x,r)) = f(x).$$

2.1) $\exists$ p.p.t Sim.

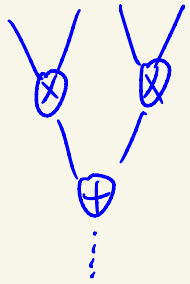
$$Sim(f(x)) \underset{p/s/c}{\simeq} \hat{f}(x,r).$$

Any f in NC_1 has an RE $\uparrow f$ in NC_0.

eg. $f(x) = \sum_i x_i \in AC_0 \in NC_1$.

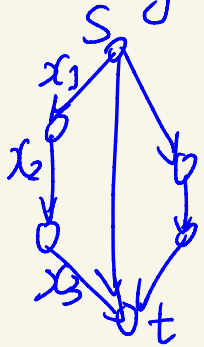
$\uparrow f(x,1) =$

Circuit



formular.

Branching Program



DAG.

图G的值是所有到t路径值之和.

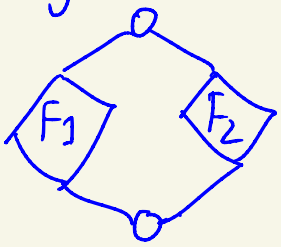
图每条路径值是各边上元素之积.

注: G的值等于连接矩阵主对角线上的边-1的Det.

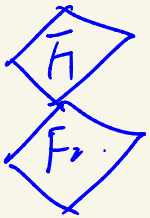
$$\begin{pmatrix} x_1 & 1 & 0 & x_1 \\ -1 & x_2 & 0 & 0 \\ 0 & -1 & x_3 & 0 \\ 0 & 0 & -1 & x_4 \end{pmatrix}$$

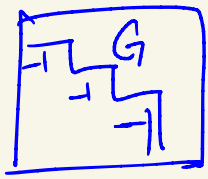
formular $\Rightarrow$ Branching Program

$F = F_1 + F_2$



$F = F_1 \cdot F_2$



$f(x) = \det$ 

$\hat{f}(x,r) =$