Lec 13 Multi-Party Computation

$f: \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3 \times \cdots \times \mathcal{X}_n \to \mathcal{Y}$ $\quad x \quad y \quad z \quad w \quad u$

Correctness

Semi-honest security against t corruptions

$\exists$ Simulator S, any subset T of size $\leq t$ any $x_1 \cdots x_n$

$$\text{View}_T(x_1, x_2 \cdots x_n) \approx S(T, (x_i)_{i \in T}, f(x_1 \cdots x_n))$$

perfect / statistical / computational

MPC for sum

$f(x_1 \cdots x_n) = \sum_i x_i$

$$
\begin{array}{c}
x_1 \leftarrow \\
\\
\\
\\
\\
\end{array}
\begin{bmatrix}
x_{11} & x_{12} & x_{13} & x_{14} & x_{15} \\
x_{21} & x_{22} & x_{23} & x_{24} & x_{25} \\
\vdots & & & \vdots & \\
x_{i1} & x_{i2} & \cdots & x_{i4} & x_{45} \\
 & & \ddots & & x_{55}
\end{bmatrix}
$$

$\qquad\qquad S_2$

$x_1 \qquad x_2 \qquad x_i \qquad x_4 \qquad x_5$

sample $x_{11} \cdots x_{15}$

$x_{11} + \cdots + x_{15} = x_1$

send x_{1j} to j-th Party

sample $x_{i1} \cdots x_{in}$

s.t. $x_{i1} + \cdots x_{in} = x_i$

send x_{ij} to j-th Party

receive x_{ji} from j-th Party

compute $\sum_j x_{ji} = S_i$

broadcast $\sum_j x_{ji} = S_i$

receive S_j

output $\sum_j S_j = f(x_1 \cdots x_n) = \sum_j x_j$

Claim: This protocol is semi-honest secure against up to $n-1$ corruptions

Secret Sharing

dealer secret x

$P_1 \quad P_2 \quad P_3 \quad P_4 \quad \cdots \quad P_n$

$$\text{share}(x) \longrightarrow (\underbrace{s_1 \quad s_2 \quad s_3 \quad s_4 \cdots s_n}_{\text{shares}})$$

threshold t

- Correctness: $\forall T \subseteq [n], |T| \geq t.\ \exists\ \text{recover}_T$
  $$\text{recover}_T((s_i)_{i\in T}) \to x$$

- Privacy: $\forall T \subseteq [n]\ |T| < t.$
  $$(s_i)_{i \in T} \equiv \text{Sim}(T)$$

Construction:

Additive secret sharing $(t = n)$

$\text{share}(x) \to$ random $s_1, \cdots s_n$

s.t. $s_1 + \cdots + s_n = x$

Shamir's threshold secret sharing

$\text{share}(x) \to (s_1 = p(1), \cdots, s_n = p(n))$

sample poly p, $p(0) = x$. degree $\leq t-1$

- Correctness

- Privacy

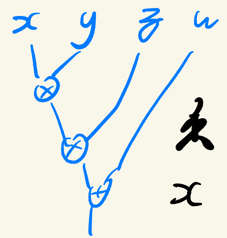
$p(w) = c_0 + c_1 w + c_2 w^2 + \cdots c_{t-1} w^{t-1}$

$c_0 = x \qquad |\mathbb{F}|^{t-1}$

$|T| = t-1 \qquad (i, s_i)$ for $i \in T \qquad |\mathbb{F}|^{t-1}$

p s.t. $p(0) = x \quad p(i) = s_i$

BGW [Ben-or Goldwasser Wigderson] Protocol is perfectly semihonest secure against $\lfloor \frac{t-1}{2} \rfloor$ corruptions

$f(\cdot\cdot\cdot) =$ 

	x	y	z		
deg-2 poly X, $X(0)=x$	$X(1)$	$X(2)$	$X(3)$	$X(4)$	$X(5)$
deg-2 poly Y, $Y(0)=y$	$Y(1)$	$Y(2)$	$Y(3)$	$Y(4)$	$Y(5)$
$\deg(XY) \le 4$	$XY(1)$	$XY(2)$	$XY(3)$	$XY(4)$	$(XY)(5)$

deg-2 P_1
$P_1(0) = c_1 \cdot XY(1)$

. . .

deg-2 P_i
$P_i(0) = c_i \cdot (XY)(i)$

send $P_i(j)$ to j-th party

deg reduction

$xy = (XY)(0)$
$= \sum_i c_i (XY)(i)$

$P = \sum_i P_i$
$P(0) = xy$

deg-2 poly Z	$Z(1)$	$Z(2)$	$Z(3)$	$Z(4)$	$Z(5)$

Round Parties $P_1 \cdots P_n$

$$P_i(x_i) \to \left((m^{(1)}_{i\to j})_{j\in[n]},\ st^{(1)}_{i} \right)$$

$$P_i\left(st^{(1)}_i,\ (m^{(1)}_{j\to i})_{j\in[n]} \right) \to \left((m^{(2)}_{i\to j})_{j\in[n]},\ st^{(2)}_i \right)$$

Randomized Encoding

$f(x)$ high-deg high-depth

$\hat{f}(x, r)$ low-degree simpler

Decoder Dec

1) Correctness

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

2) $\exists$ Simulator S. $\forall x$

$$\hat{f}(x,r) \equiv S(f(x))$$

randomness from r randomness from S

$f(x_1, \ldots x_n)$ assume RE

$\hat{f}(x_1, \ldots x_n, r)$

Want: MPC for f

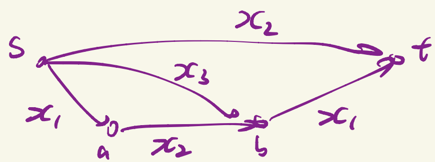
MPC: $(x_1, r_1) \quad (x_2, r_2) \quad \ldots \quad (x_n, r_n) \mapsto \hat{f}(x_1 \ldots x_n, \sum_i r_i)$

Toy Example $f(x_1 \dots x_n) = x_1 + x_2 + \dots + x_n$

$\hat{f}(x_1\ r_1\ x_2\ r_2\ x_3\ r_3\ x_4\ r_4\ \dots) \in NC_0$

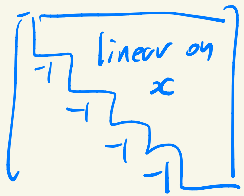
$= (x_1 + r_1,\ -r_1 + x_2 + r_2,\ -r_2 + x_3 + r_3\ \dots)$

NC_1 Circuit $\longrightarrow$ poly-size Branching Program

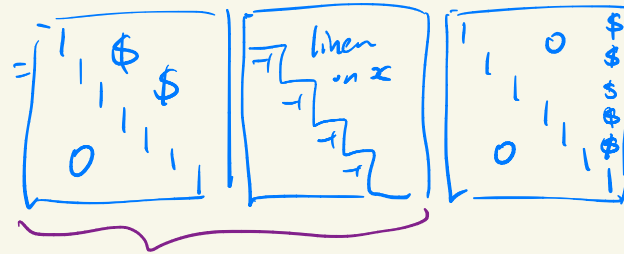


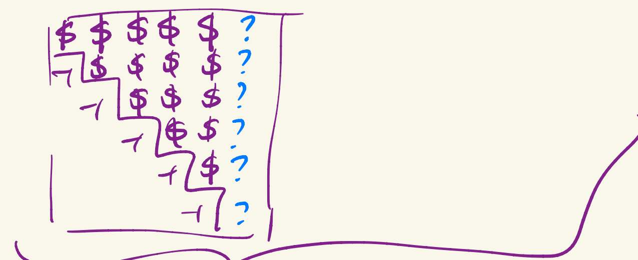
$$x_2 + (x_1 x_2 + x_3) x_1 = \det \begin{array}{c|c} & a \quad b \quad t \\ \hline \begin{array}{c} s \\ a \\ b \end{array} & \begin{bmatrix} x_1 & x_3 & x_2 \\ -1 & x_2 & \\ & -1 & x_1 \end{bmatrix} \end{array}$$

$f(x) = \det$

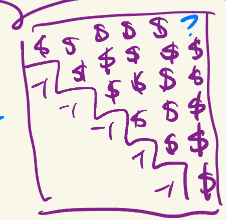


$\hat{f}(x, r) =$





$f(x) = \det$



$\deg(\hat{f}) = 3$

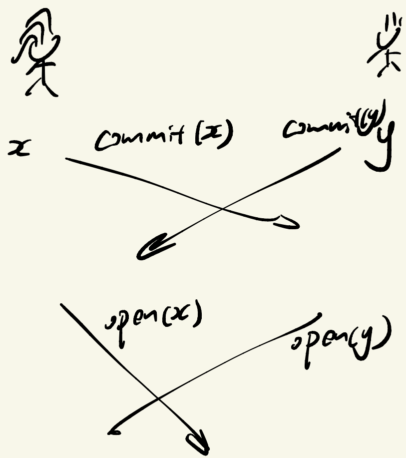
Malicious Security.

Model: { P2P secure channel
broadcast } + #corruptions $< \frac{n}{3}$

{ rushing
non-rushing }

Alice Bob

$(x, y) = x \oplus y$



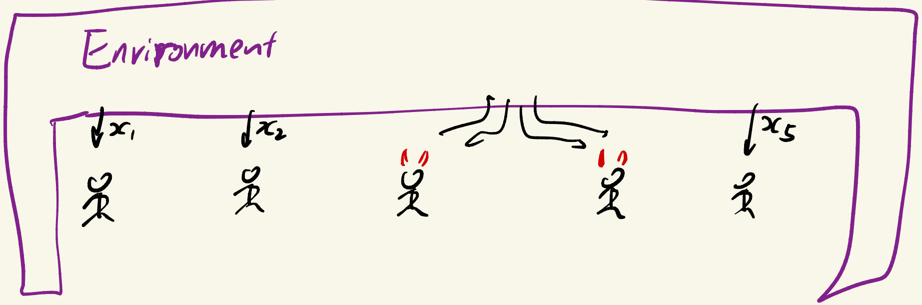
Security definition {

GOD, full security

guarantee output delivery

Full Security
= GOD security

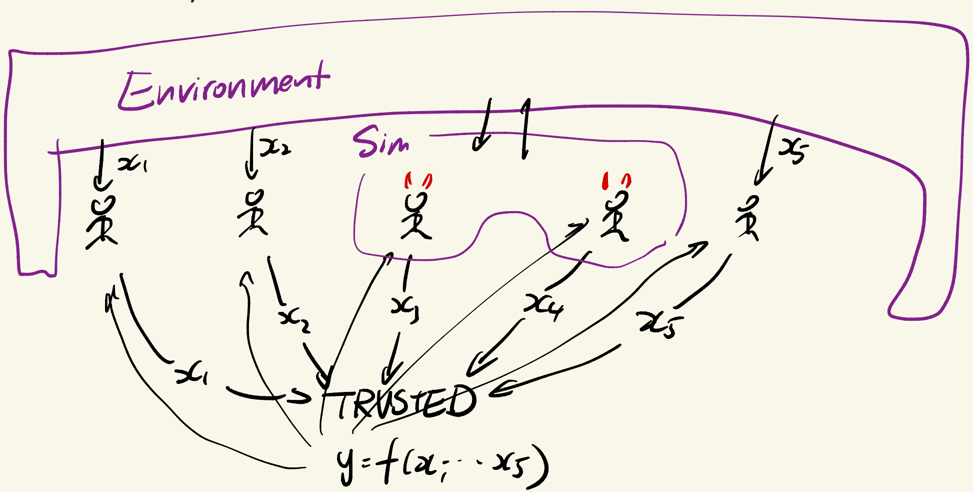
REAL WORLD



$$(\text{View}_E,\ \text{View}_{\text{Corrupted}},\ \text{Output of honest parties})$$

$$\approx_{SS}$$

IDEAL WORLD $(\text{View}_E,\ \text{Sim},\ \text{Output of honest parties})$



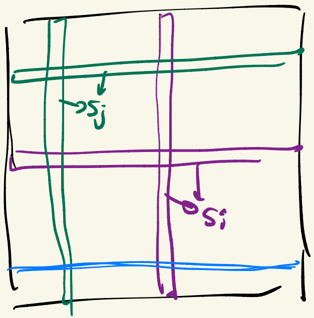
VSS $\Rightarrow$ Full Security

\# corruptions $\leq 1/_{3} n$, assume broadcast

verifiable secret sharing

share $(x) \rightarrow$ poly $P(i,j)$, 1) deg(P) small

2) $P(0,0) = x$



$(S_1 \ldots S_i \quad S_j \ldots S_n)$

$S_i = P(i,\cdot)$, $P(\cdot,i)$

$S_j = P(j,\cdot)$, $P(\cdot,j)$

1) Check low-degree

Party i&j check $P(i,j) = P(i,j)$, & $P(j,i) = P(j,i)$

Broadcast if disagree.

2) Find large set S st. $\forall i,j \in S$ Party i&j agree

|S| small, replace share by zeros

|S| large, if $i \notin S$, discard local share

recover "correct" local share using ECC

High

Security

Low

Full - Security = GOD

Security w/ Abort

Security w/ Selective Abort

Privacy w/ Knowledge of Output

~~Privacy~~

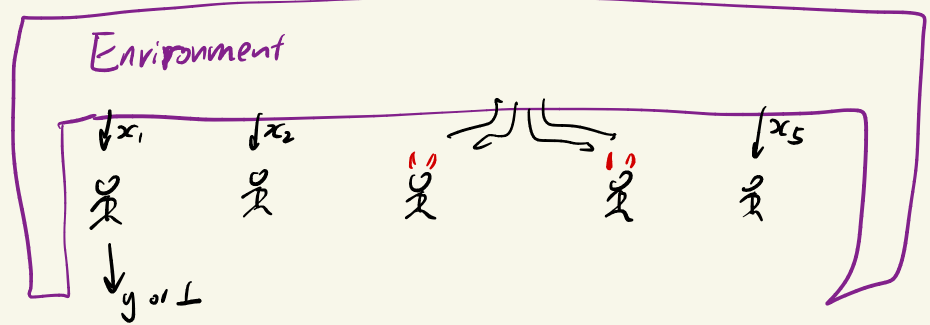
Broadcast

Broadcast Signature

HW

Security w/ Abort

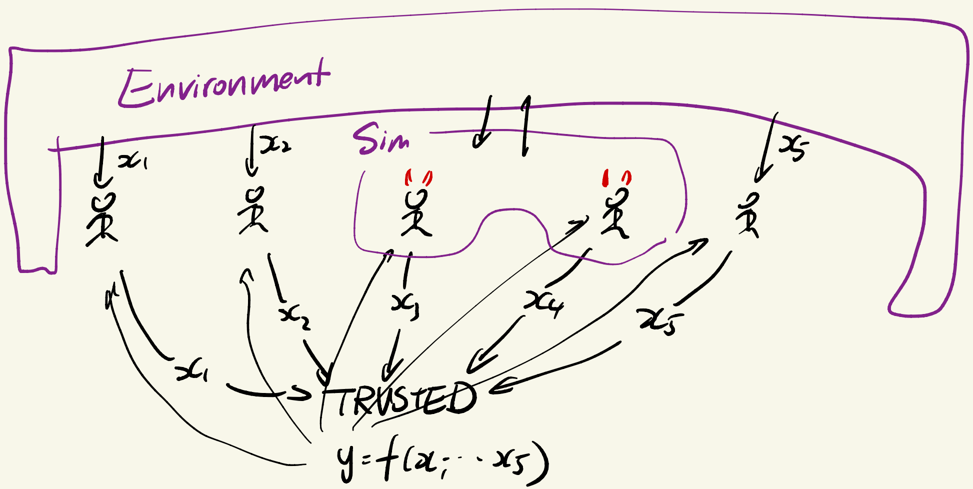
REAL WORLD



$$\frac{(\text{View}_E,\ \text{View}_{\text{Corrupted}},\ \text{Output of honest parties})}{(\text{View}_E,\ \text{Sim},\ \text{Output of honest parties})}$$

SS

IDEAL WORLD

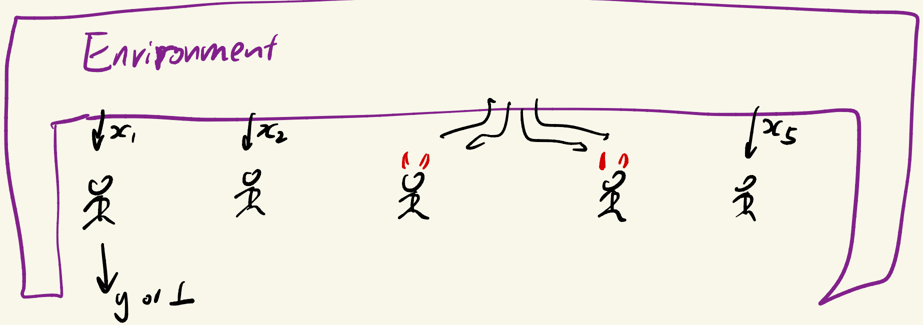


TRUSTED

1) receive x_i from i-th Party
2) send $y \to$ Sim
3) receive "PASS" "ABORT" from Sim
4) send $\begin{cases} y & \text{"PASS"} \\ \perp & \text{"ABORT"} \end{cases}$ to i-th party

Security w/ Selective Abort

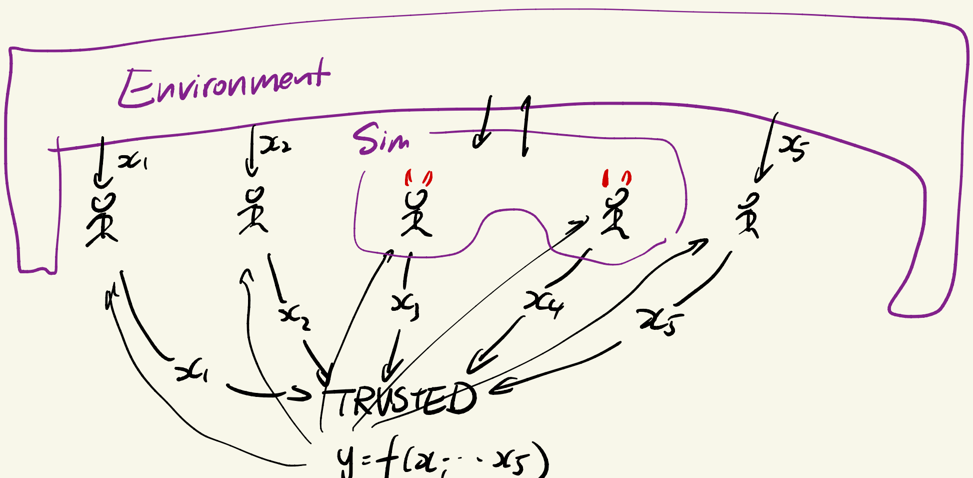
REAL WORLD



$(View_E, View_{corrupted}, \text{Output of honest parties})$

SS

IDEAL WORLD $(View_E, \text{'Sim'}, \text{Output of honest parties})$



TRUSTED

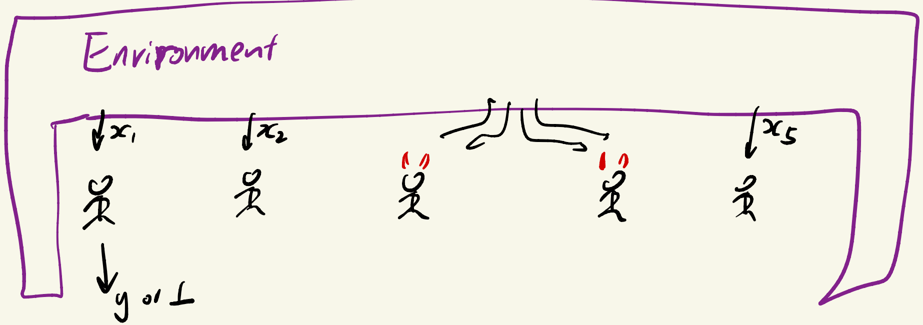
1) receive x_i for i-th Party

2) send $y \to$ 'Sim'

3) receive $\vec{b} \in \{0,1\}^n$ from 'Sim'

4) send $\begin{cases} y & b_i = 0 \\ \perp & b_i = 1 \end{cases}$ to i-th party

Security w/ Selective Abort

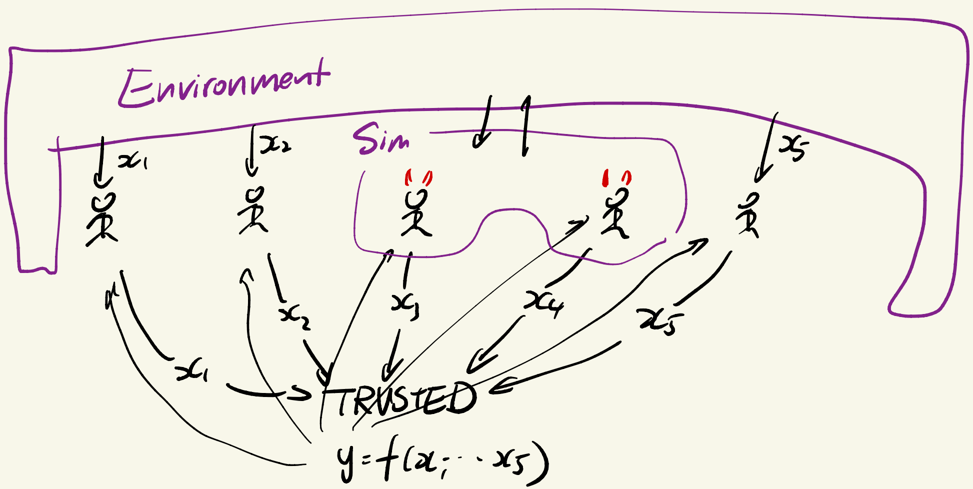


REAL WORLD

$\left(\text{View}_E ,\ \text{View}_{\text{Corrupted}} ,\ \text{Output of honest parties} \right)$

SS

IDEAL WORLD $\left(\text{View}_E ,\ \text{'Sim'} ,\ \text{Output of honest parties} \right)$



TRUSTED

1) receive x_i for i-th party
2) send $y \rightarrow$ 'Sim'
3) receive y'.
4) send y' to i-th party