- Scribes?
- lecture recording

SPDZ

$[x]$ - additive sharing, i.e., P_i holds x_i, $x_1 + \cdots + x_n = x$

- homomorphic w.r.t. addition, & multiplication by constant i.e., given $[x]$, $[y]$, parties can locally compute $[x+y]$ and $[a \cdot x]$

Say parties hold shares $[a]$, $[b]$, $[c]$, $c = ab$

They can multiply $[x]$, $[y]$ as follows:

1. $\text{Open}(\underbrace{[x-a]})$, $\text{Open}(\underline{[y-b]})$
2. $[z] = [c] + (x-a)\cdot[b] + (y-b)\cdot[a] + (x-a)(y-b)$
   $= [xy]$

Three stages in SPDZ protocol:

1. Initial set-up (once and for all)
2. Preprocessing phase (per execution)
3. Online phase

authenticate the shared value

For some global key α, $\langle x \rangle = ([x], [\alpha \cdot x])$

each party could reveal x_i, $(\alpha x)_i$

Still homomorphic! $\langle x \rangle$, $\langle y \rangle$, parties can locally compute

$$\langle x \rangle = ([x], [\alpha x]), \quad \langle y \rangle = ([y], [\alpha y])$$

$$\Rightarrow ([x+y], [\alpha x + \alpha y]) = ([x+y], [\alpha(x+y)])$$

Parties initially hold $[\alpha]$, $\langle a \rangle, \langle b \rangle, \langle c \rangle$, $c = ab$

Given $\langle x \rangle, \langle y \rangle, \langle a \rangle, \langle b \rangle, \langle c \rangle$, Then parties can compute $\langle xy \rangle$ just like before

1. Open$(\langle x-a \rangle)$, Open$(\langle y-b \rangle)$
2. locally compute $[z] = [c] + (x-a)[b] + (y-b)[a] + (x-a)\cdot(y-b)$

   $[\alpha z] = [\alpha c] + (x-a)[\alpha b] + (y-b)[\alpha a] + \downarrow \; [\alpha]$

Protocol

1. Assume for each input, parties hold $\langle r \rangle$
   Open$(\langle r \rangle)$ to P_i, then P_i sends $x - r$, all parties adjust their shares $\Rightarrow \langle x \rangle$
2. Run semi-honest protocol on authenticated shares of inputs
3. let $x_1, \dots, x_n$ be all opened values, let $\langle y \rangle$ be the output
   generate some random r, set $x = \sum x_i r^i$
4. P_j commits to $\sum (\alpha x_i)_j r^i = \gamma_j$
   Commits to y_j, $(\alpha y)_j$
5. Open α // see below
6. Parties reveal γ_j; check that $\alpha \cdot x \stackrel{?}{=} \sum \gamma_j$
7. Parties reveal y_j, $(\alpha y)_j$; check that $\alpha \cdot \sum y_j = \sum (\alpha y)_j$

Consider cheating adversary. Let $\hat{x}_1, \ldots, \hat{x}_N$ be the correct values, and $x_1, \ldots, x_N$ the values opened. Let $\hat{x} = \sum \hat{x}_i r^i$, $x = \sum x_i r^i$.
If $(x_1, \ldots, x_N) \neq (\hat{x}_1, \ldots, \hat{x}_N)$, then $\Pr_r[\hat{x} = x] \leq N/|\mathbb{F}|$.
(Consider polynomial $\Delta(R) = \sum(\hat{x}_i - x_i)R^i$, which has $\leq N$ roots.)
If $\hat{\gamma} = \alpha \cdot \hat{x}$, then adversary can set $\gamma = \hat{\gamma} + \varepsilon$ for arbitrary ε.
But if $\hat{x} \neq x$, then $\Pr_\alpha[\alpha \cdot x = \hat{\gamma} + \varepsilon = \alpha\hat{x} + \varepsilon] \leq 1/|\mathbb{F}|$.

α can be shared as $\left([\alpha], \{(\beta_i, \underline{[\beta_i \alpha]})\}_{i=1}^{n} \right)$

Initial setup: pk for a somewhat homomorphic encryption (SHE) scheme, with threshold decryption

SHE scheme:

$$\mathrm{Enc}_{pk}(x),\ \mathrm{Enc}_{pk}(y) \Rightarrow \mathrm{Enc}_{pk}(x+y)$$

$$\mathrm{Enc}_{pk}(x),\ \mathrm{Enc}_{pk}(y) \Rightarrow \mathrm{Enc}'_{pk}(xy)$$

$$\mathrm{Enc}'_{pk}(x),\ \mathrm{Enc}'_{pk}(y) \Rightarrow \mathrm{Enc}'_{pk}(x+y)$$

P_i: $\mathrm{Enc}_{pk}(\alpha_i) \longrightarrow \mathrm{Enc}_{pk}(\alpha)$ $\quad \alpha = \sum \alpha_i$

$\mathrm{Enc}_{pk}(a_i) \longrightarrow \mathrm{Enc}_{pk}(a)$ $\quad a = \sum a_i$

$\mathrm{Enc}_{pk}(b_i) \longrightarrow \mathrm{Enc}_{pk}(b)$

$\longrightarrow \mathrm{Enc}'_{pk}(ab)$

$\mathrm{Enc}'_{pk}(\Delta_i) \longrightarrow \mathrm{Enc}'_{pk}(\Delta)$

$\longrightarrow \mathrm{Enc}'_{pk}(ab + \Delta)$

$\longrightarrow ab + \Delta$

P_1: $(ab+\Delta) - \Delta_1$

$P_{i, i>1}$: $-\Delta_i$

$\underline{t < n/2}$

$[x]$ = $(t+1)$-out-of-n Shamir sharing

Given $(x_1, \ldots, x_n)$

$(y_1, \ldots, y_n)$

Parties compute $(x_1y_1, \ldots, x_ny_n)$

then P_i shares x_iy_i using a degree-t poly.

parties add up their shares.

define $\mathcal{F}^{\Delta}_{\text{mult}}$

Idea: parties share $[\alpha]$; compute f on $\{[x_i]\}$ and $\{[\alpha x_i]\}$.

multiplication: $[x], [y], [\alpha x], [\alpha y]$

$\Longrightarrow$ $[xy], [\alpha xy]$

At the end of the protocol, let $\{[z_i], [\alpha z_i]\}_{i=1}^{N}$ be all values output by mult. gate

generate random $r_1, \ldots, r_N$

Compute $\underline{[v] = \sum r_i [z_i], \quad [w] = \sum r_i [\alpha z_i]}$

Open α

Check $[w] - \alpha[v] \stackrel{?}{=} [0]$

Open outputs

$[z_i + \Delta], \quad [\alpha z_i + \Delta']$

if $(\Delta, \Delta') \neq (0,0)$ $\quad \Pr_{\alpha}[\alpha z_i + \Delta' = \alpha \cdot (z_i + \Delta)] = 1/|\mathbb{F}|$