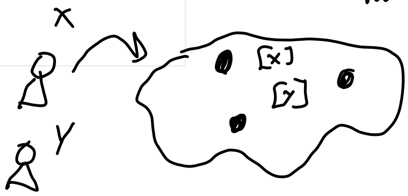
MPC

Monday, October 25, 2021 3:54 PM

Recap of MPC:

- n servers, up k of them can fail,
  we use secret sharing of degree k.



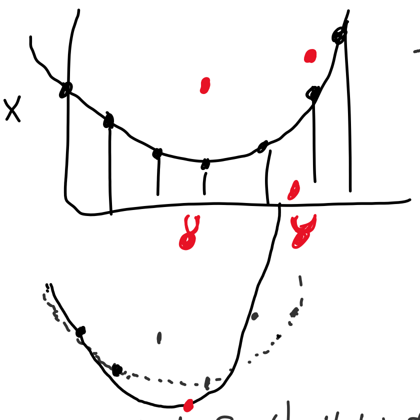
$a_0 = x \quad a_1 \overset{\$}{\leftarrow} \mathbb{F}_p \; \dots \; a_k \overset{\$}{\leftarrow} \mathbb{F}_p.$

- Secret Share(x): as client
  Sampling φ uniformly (among p^k possibilities)
  s.t. $\varphi(0) = x$ and φ is degree-k
  Send $\varphi(i)$ to server S_i as $[x]^{(i)}$

- Open$([x])$: as server S_i
  Send $[x]^{(i)}$ to each other server
  Receive n initial shares from other servers $[x]^{(j)}$
  Interpolate a polynomial φ s.t. $\varphi(j) = [x]^{(j)}$
  output $x = \varphi(0)$.

Robust Reconstruction.

- Suppose the servers that fail (up to k)
  they return invalid shares during Open
- Can we ensure we get the correct value anyway?



$k = 2$

* Only one subset of 4 that works. ?

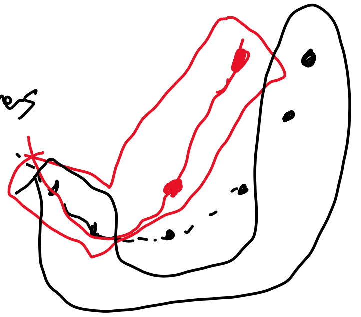
- Find a large enough subset. ~~4~~? 5?
- Potentially two subsets each intersecting 4 points.
- If we can find a deg k poly intersecting

2K+1 received shares.

⇒ we can conclude it is the correct one.

- Among 2k+1 received shares, at most K come from malicious nodes. So at least K+1 are correct shares. And K+1 correct shares uniquely determine the correct φ.

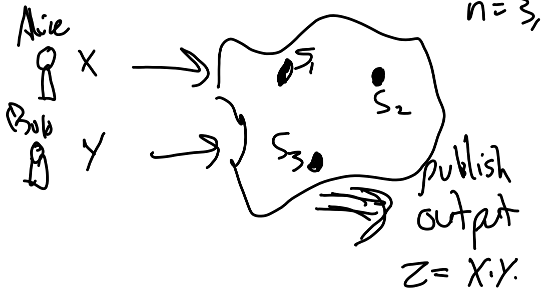
- $n \geq 2K+1$ is the minimum number of servers relative to fault tolerance K for which robust interpolation works.

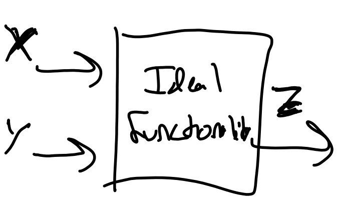


- $n \geq 3K+1$ is the minimum to ensure guaranteed output
  (if the 2K+1, first shares aren't successful, wait for more and try again.
  Output once some subset of 2K+1 received shares lie on a deg K poly.).

Simulation Security for MPC.

$n=3$, $K=1$, semihonest





View can be simulated given just z

```
Input: x, y
Preproc: [a], [b], [ab].
Procedure:
    Alice  SecretShares(x)
    Bob    SecretShares(y)
    Servers:
        D := Open([x] - [a])
        E := Open([y] - [b])
        [z] := DE + . . + [ab]
        output z := Open([z])
```

Beaver mul

☆ Alt interpretation:
flip a bit, either produce the real view, or the simulation.
These are indistinguishable.

☆ for all x_L, y_L, x_R, y_R, s.t. $y_L \cdot x_L = y_R \cdot x_R$.

$$View_L \approx View_R$$

- What is the view of S_1 in this protocol?

— enumerate everything S_i sees. Total $\mathbb{F}_p$.

Server i sees:

- $[x]^{(i)}, [y]^{(i)},$ 2x
- $[a], [b], [ab]$ 3x
- φ_D from reconstruction 2x (deg 1 poly)

  $\varphi_D(i) = [x-a]$ 2x
- φ_E
- φ_Z 2x

Total 11x $\mathbb{F}_p$ elems.

— Give a Pr distribution DoF

$\varphi_D(i) = [x-a]$ -1

$\varphi_E(i) = [y-b].$ -1

$\varphi_Z(i) = DE + \cdots [ab]$ -1

$\varphi_Z(0) = Z$ -1

In total, p^7 possible views, all equally likely.

— How can it be simulated given Z.

given prob dist. above, sample in any order that satisfies constraints.

$S(Z)$:

~~$\varphi_Z \xleftarrow{\$}$ deg-1 polys.~~