Tolerating ACTIVE Adversaries (Byzantine)

→ t Byzantine faults

use Byzantine Agreement ($n > 3t$) → To simulate Broadcast

perform verifiable secret sharing.

Protocol:

Secret $s$

Choose a random symmetric* bi-variate polynomial of degree $t$ (each)

$$Q(x,y) = \sum_{i=0}^{t} \sum_{j=0}^{t} \alpha_{ij} x^i y^j$$

symmetric ⇒ $Q(a,b) = Q(b,a)$

$Q(0,0) \Rightarrow$ secret

- Send $Q(x, i)$ to player $i$

  ↳ share is a $t$-degree polynomial

Verification.

→ Each $P_i$ checks if $Q(x,i)$ is a $t$-deg polynom.

→ For each pair of players $P_i, P_j$

Check

$$Q(i,j) = Q(j,i)$$

→ if all match; we are done; share secrets using the poly.

→ else

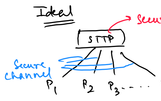
if $P_i$ & $P_j$ don't match

- one of $\{P_i, P_j, \text{sender}\}$ is faulty
- remove all 3 // ⟶ continue protocol between remaining three.

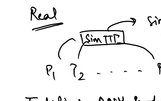
$n > 3t \Rightarrow n-3 > 3(t-1)$

Defining a problem in Third party model

Ideal




Real




To define ANY problem. ('SIM definition')

ⓐ write protocol in IDEAL world ($\Psi_{ideal}$) (Easy)

Ex

→ Comm betw $i$ & $j$

⇒ $i$ sends to STTP

⇒ STTP sends to $j$

→ Election

⇒ $P_1, \dots P_n$ send vote to STTP

⇒ STTP counts votes declares winner

ⓑ real world protocol ($\Psi_{real}$) is secure

if

→ $\forall$ real world adversaries $\mathcal{A}$

$\exists$ ideal world adversary $S$ s.t. (same nodes are corrupted)

$$view(S) \equiv view(\mathcal{A})$$
$$\| \qquad\qquad \|$$
$$\Psi_{ideal} \qquad \Psi_{real}$$

most textbooks do not use SIM definition, because showing that views are same is very hard

use IND Definition **

↳ harder to comm with the definition, easier to prove.

consider a subroutine running inside main

```
main():
    subroutine()
```

if we have correctness proof for subroutine & " " " main

⇒ we have correctness proof for the entire program

However this does NOT work for security.

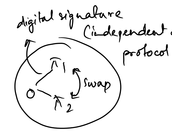
say you have PRP $P$

subroutine $(x) = p(x)$

main. ⇒ $p^{-1}(x)$

main + subroutine ⇒ $p^{-1}(p(x)) = x$

∴ we have a SIM definition protocol which works well when isolated, but when is in contact with other protocols, can be insecure




U-SIM (Universal SIM definⁿ)

ⓐ write protocol in IDEAL world ($\Psi_{ideal}$) (Easy)

Ex

→ Comm betw $i$ & $j$

⇒ $i$ sends to STTP

⇒ STTP sends to $j$

→ Election

⇒ $P_1, \dots P_n$ send vote to STTP

⇒ STTP counts votes declares winner

ⓑ real world protocol ($\Psi_{real}$) is secure

if

→ $\forall$ real world adversaries $\mathcal{A}$ & $\forall$ Environments $\mathcal{E}$.

$\exists$ ideal world adversary $S$ s.t. (same nodes are corrupted)

$$view(S) \equiv view(\mathcal{A})$$
$$\| \qquad\qquad \|$$
$$\Psi_{ideal} \qquad \Psi_{real}$$

Timing → Synchrony, Asynchrony

Protocol → ITM, RPC,

Network → Undirected Graph, Di graph, Spl. Graph, Hypergraph ...

Adversary → Passive / Active; Threshold / General; Mobile / Adaptive / Static

Simulⁿ Strength → Perfect, Statistical, Computational ...

System?

Quantum?

Relativistic?

Noisy channel?