Scribes?

Lecture Recording

No class next week

Midterm

GMW II Compiler

Broadcast / Byzantine agreement

Security with abort

Standard model when $t < n/2$ and broadcast available can ensure that only one designated party can abort (if they are corrupted)

Full security

Malicious parties do not have the option of aborting

The ideal functionality

Standard model when $t < n/2$ and broadcast available or $t < n/3$
GMJ II Compiler

Start with semi-honest protocol \( \Pi \), secure against \( T < \frac{n}{2} \) parties

Shamir's secret sharing \( \Rightarrow (t+1)\) out of \( n \) sharing

\[ \text{Committed Verifiable secret sharing (VSS)} \]

\[ \forall i \] \( P_i \times x_i \)

\[ \text{Public information:} \]

\[ \text{Com} = \text{Com}(x_1, y_1), \ldots, \text{Com}(x_n, y_n) \]

Each party \( P_i \) holds:

- \( x_i, y_i \)

\( P_i \) holds:

- \( x_1, x_2, \ldots, x_n, y_1, \ldots, y_n \)

\[ \tilde{G}_{\text{VSS}}(x_1, x_2, \ldots, x_n) = (\text{Com}(x_1, y_1), \text{Com}(x_2, y_2), \ldots, \text{Com}(x_n, y_n)) \]

Compiled protocol \( \Pi' \)

1. Parties compute \( \tilde{G}_{\text{VSS}} \) using a secure-with-abort protocol;
   once per party
   - if some \( P_i \) misbehaves, kick them out and use a
     default input for them

2. Parties do the same for a random version of \( \tilde{G}_{\text{VSS}} \), once per party
   - if \( P_i \) misbehaves, kick it out

3. Run \( \Pi' \) using the committed inputs and randomness, giving \( 2k \) proof
   of correctness after each msg.
- If $P_i$ fails when giving some $2k$ proof,
  - each party broadcasts their share of $P_i$'s input/randness,
  - plus the corresponding $P_i$'s
  - parties reconstruct $P_i$'s input/randness from $2k$ correct shares
  - parties run $TT$ on behalf of $P_i$ from then on

Broadcast channel

Parties can realize a broadcast channel using a broadcast protocol

Broadcast protocol

Protocol run by parties $P_1, \ldots, P_n$ with designated $P^* \in \{P_1, \ldots, P_n\}$
acting as a sender with initial input $m$

[Validity] If $P^*$ is honest, then all honest parties output $m$

[Consistency] All honest parties should output the same value

Broadcast protocol $\equiv$ Realizing $f_{\text{Beast}}$ with full security

* non-adaptive setting,
* $\geq 3$ corrupted parties (need private broadcast otherwise)
Byzantine agreement protocol

Protocol run by parties $P_1, ..., P_n$ where each $P_i$ has initial
input $m_i$.

(Consistency) All honest parties output the same value.

(Validity) If all honest parties hold the same initial value $m_i$,
then all honest parties output $m_i$.

For $t < n/2$, $BA \Rightarrow$ broadcast

broadcast $\Rightarrow$ BA

$BA$ only makes sense for $t < n/2$,
whereas broadcast makes sense even for $t < n$.

With no prior setup, $BA$/broadcast are impossible if $t \geq n/3$.

Consistency $\Rightarrow m_2 = m_3$

Validity $\Rightarrow m_3 = 1, \quad m_2 = 0$ \quad (contradiction)