SaUCy Reference: Reliable Broadcast

1 Overview

Adaptively secure broadcast [2]. Bracha [1]. We assume a static adversary.

2 Ideal Functionalities

Functionality $\mathcal{F}_{\text{ACAST}}$

$\mathcal{F}_{\text{ACAST}}$ interacts with an adversary $\mathcal{S}$ and a set $\mathcal{P} = \{P_1, \ldots, P_N\}$ of parties.

1. Upon receiving (Bcast, sid, m) from P_s:
   - If P_s is honest, then leak $(\mathsf{Bcast}, sid, P_s, m)$ and, for each P_i in $\mathcal{P}$, send $(\mathsf{Bcast}, sid, P_s, m)$ **eventually**.
   - If P_s is corrupted, then send nothing.

3 Protocol Definition

Protocol Π_{Bracha}

Π_{Bracha} interacts with a set $\mathcal{P} = \{P_1, \ldots, P_N\}$ of parties and can tolerate up to t failures.

1. Upon receiving (Value, v) from P_i, send $(\mathsf{Initial}, v)$ to all parties in $\mathcal{P}$.
2. Upon receiving an $(\mathsf{Initial}, v)$ message or $\lceil \frac{N+t}{2} \rceil$ (Echo, v) messages or $\lceil \frac{t+1}{2} \rceil$ (Ready, v) messages, send (Echo, v) to all parties in $\mathcal{P}$.
3. Upon receiving $\lceil \frac{N+t}{2} \rceil$ (Echo, v) messages or $\lceil \frac{t+1}{2} \rceil$ (Ready, v) messages, send (Ready, v) to all parties in $\mathcal{P}$.
4. Upon receiving $\lceil \frac{t+1}{2} \rceil$ (Ready, v) messages, accept v.

4 Protocol Emulation

Theorem 1. *Protocol Π_{Bracha} t-securely realizes the functionality $\mathcal{F}_{\text{ACAST}}$ for $t < N/3$.*

Proof sketch. Let $\mathcal{A}$ be an adversary attacking Π_{Bracha}. We build a corresponding simulator $\mathcal{S}$ as follows.

Simulator $\mathcal{S}_{\text{ACAST}}$

1. Run a copy of the real world execution in a sandbox.
2. Whenever $\mathcal{A}$ requests to corrupt some $P_i \in \mathcal{P}$, corrupt P_i and send the internal state of P_i to $\mathcal{A}$. Hereafter, $\mathcal{S}$ has P_i follow $\mathcal{A}$'s instruction.
3. Whenever $\mathcal{A}$ sends a message to the environment $\mathcal{Z}$, $\mathcal{S}$ forwards this message to $\mathcal{Z}$.
4. Wait until an honest party P_i outputs a value m_i, and send this value to $\mathcal{F}_{\text{ACAST}}$.

Verifying that $\text{EXEC}[\Pi_{\mathsf{Bracha}}, \mathcal{A}, \mathcal{Z}] \approx \text{EXEC}[\mathcal{F}_{\text{ACAST}}, \mathcal{S}, \mathcal{Z}]$ is left as an exercise to the reader because I have no idea what I'm doing. □

References

1. Gabriel Bracha. Asynchronous byzantine agreement protocols. *Information and Computation*, 75(2):130–143, 1987.
2. Juan A Garay, Jonathan Katz, Ranjit Kumaresan, and Hong-Sheng Zhou. Adaptively secure broadcast, revisited. In *Proceedings of the 30th annual ACM SIGACT-SIGOPS symposium on Principles of distributed computing*, pages 179–186. ACM, 2011.