SaUCy Reference: Reliable Broadcast

1 Overview

Adaptively secure broadcast [2]. Bracha [1].

2 Ideal Functionalities

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

$\mathcal{F}_{\text{BC}}$ 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_i, send $(\text{Bcast}, sid, P_i, m)$ to all parties in $\mathcal{P}$ and to $\mathcal{S}$.

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

$\mathcal{F}_{\text{RBC}}$ 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_i, leak $(\text{Bcast}, sid, P_i, m)$ to $\mathcal{S}$.
2. Upon receiving m' from $\mathcal{S}$, do:
   - If P_i is corrupted, send $(\text{Bcast}, sid, P_i, m')$ to all parties in $\mathcal{P}$.
   - If P_i is not corrupted, send $(\text{Bcast}, sid, P_i, m)$ to all parties in $\mathcal{P}$.

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_i, leak $(\text{Bcast}, sid, P_i, m)$ to $\mathcal{S}$.
2. Upon receiving m' from $\mathcal{S}$, do:
   - If P_i is corrupted, send $(\text{Bcast}, sid, P_i, m')$ to all parties in $\mathcal{P}$.
   - If P_i is not corrupted, send $(\text{Bcast}, sid, P_i, m)$ to all parties in $\mathcal{P}$.

3 Protocol Definition

Protocol Π_{Bracha}

Π_{Bracha} interacts with a set $\mathcal{P} = \{P_1, \ldots, P_n\}$ of parties.

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

4 Protocol Emulation

Simulator $\mathcal{S}_{\mathsf{BC}}$

PROOF SKETCH Sketch simulation proof here. □

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.