Team Rap: Rasmus Jørgensen (201909451), Mathias Weller (201907948) & Anna Blume (201907691)

Hand-in 5 (DISSY)

In DolevStrong, if the sender is Byzantine corrupted it can force the honest parties to send a large number of messages by sending signed (bid;m) for a large number of different m. Make an improved version of the protocol where you limit how many messages the honest parties can be forced to send. Argue that the protocol is still secure.

Protokol:
Den nye protocol følger Dolev-Strong indtil en ærlig receiver har accepteret mere end én besked. Når den anden unikke besked bliver accepteret (så $|Accepted| > 1$) signeres og broadcastes den som sædvanligt, men derfra sender den pågældende receiver ikke flere beskeder på netværket før den til sidst laver sit output (som altid vil være NoMsg).

Termination:
Protokolen terminerer i kraft af at DolevStrong terminerer, og vi har stadig præcis n + 1 runder, hvorefter, hvert ærligt party beslutter kommer med et output i samme runde.

Validity:
Hvis vi har en ærlig sender S, vil der kun være én korrekt signeret besked i netværket, og derfor vil vores protokol opføre sig fuldstændig som den oprindelige DolevStrong, og have validity i kraft af at DolevStrong har validity.

Agreement:
Hvis kun én besked bliver sendt af en ærlig sender, vil alle stadigvæk modtage og sende denne ene besked videre, så alle modtager den alene, og der er agreement. Hvis senderen derimod er uærlig, og arbejder sammen med et antal andre adversaries, vil en eventuel besked nr. 2 på et tidspunkt blive sendt til mindst ét ærligt party. Når dette sker, vil det være den første eller anden besked den ærlige receiver ser, og den vil derfor stadigvæk broadcaste beskeden og sikre, at alle andre ærlige også ser mindst to beskeder. Den ærlige receiver vil også på et tidspunkt modtage besked nr. 1 (eller har allerede modtaget den), og have $|Accepted| > 1$. Kommer der en besked nr. 3, vil den ærlige receiver vide at alle andre ærlige receivers har set de to første den selv har set, og kan godt lade være med at fortælle de andre om den tredje besked, da alle nu alligevel vil give NoMsg.