Homework

April 9, 2017

Chose and answer at least one of the following (overlapping) questions:

1. Prove or disprove: The notions of Byzantine agreement of Definitions 1 and $1'$ are equivalent.
2. Prove or disprove: Protocol BA' satisfies Definition 1.
3. Prove of disprove: Protocol $BA\star$ satisfies Definition $1'$.

Protocol BA' is our rendition of the Dolev-Strong BA protocol, and protocol $BA^\star$ has not yet been presented (so feel free to choose and solve Question 3 after $BA^\star$ has been presented). In both protocols the adversary is assumed to be polynomially bounded.