

CSCI 4510/6510: Distributed Systems and Algorithms - Homework 4 Problem Set

Due Sunday, December 8, 2024 at 11:59pm in Gradescope

Submission requirements

- Homework must be typed and submitted as a pdf file in Gradescope.
- If you include figures, they may be hand-drawn or digitally created.
- Solutions must be relevant to your specific code submission to receive full credit. You should reference and/or explain key details of your implementation to illustrate your point when applicable.
- Solutions must be self-contained. The grader should not need to check your program code to grade the solutions.
- You may discuss the problems and solutions with others, but you must write up your solutions independently.

Required for CSCI 4510 and 6510

Problem 1 Give a proof that the Dolev-Strong algorithm satisfies property (IC2) for Byzantine Agreement for any number of traitors less than or equal to m .

Problem 2 Suppose the system always has at least one honest site and that $m = n - 1$. In your implementation, are there any circumstances in which an honest site issues a proposal for a log slot, but that log slot is not filled at that site? Answer YES or NO and justify your answer. You should consider all types of Byzantine behavior, not just the behaviors you implemented for this homework.

Problem 3 In this homework, we assumed that there is exactly one proposed log entry for each log slot. Suppose we remove this restriction and allow multiple sites to propose different log entries for a single log slot. How would you update your implementation so that it still guarantees (IC1) and (IC2)? Be sure to justify why your updated implementation satisfies these two properties.

Required for CSCI 6510 only

Problem 4 Give a proof sketch that shows that the Dolev-Strong algorithm satisfies property (IC1) for Byzantine Agreement for any number of traitors less than or equal to m .