

Exercise 7

1 SINTRA and secure distributed DNS

Read the papers on SINTRA [CP02] and on its application to securing a distributed DNS implementation [CS04]. They will be discussed in the next lecture:

[CP02] C. Cachin and J. A. Poritz, *Secure intrusion-tolerant replication on the Internet*, Proc. International Conference on Dependable Systems and Networks (DSN-2002), June 2002, pp. 167–176.

[CS04] C. Cachin and A. Samar, *Secure distributed DNS*, Proc. International Conference on Dependable Systems and Networks (DSN-2004), June 2004, pp. 423–432.

2 Atomic broadcast using a trusted leader

As mentioned in Section 6.5, atomic broadcast can be implemented using a sequence of agreements on messages to be delivered. This approach is relatively slow because it involves expensive public-key cryptography in the critical path of every atomic message delivery.

An alternative is to resort to one of the cheaper broadcast primitives, like consistent or reliable broadcast; however, they only guarantee liveness if the sender is honest.

- a) Assume the system contains one party P_ℓ that is trusted (i.e., cannot be corrupted by the adversary and does not fail) and design an atomic broadcast protocol for this setting (assuming $n > 3t$).
- b) How can this approach be extended to an atomic broadcast protocol that avoids the strong assumption on P_ℓ ? (Sketch a solution using the rotating coordinator paradigm.)