A Note on Fault-tolerant Distributed Algorithms

Sourav Das
souravd2@illinois.edu

April 2022

Abstract

This document list some problems that I have thought about and potentially have a solution to. We decided not to write a formal write-up about them for various reasons.

Asynchronous Distributed Key Generation

- ADKG with expected round complexity of $O(\log \kappa)$ and computation cost of $O(\kappa n^2)$. Here κ is the statistical security parameter.
- Low-threshold ADKG with expected round complexity of $O(1)$ and computation cost to $O(n^2)$.
- ADKG with expected round complexity of to $O(1)$.

Computational coin tossing protocol

- An one-shot partially synchronous coin-tossing protocol with $n = 3t + 1$ and expected communication cost of $O(c \cdot n^{2+1/c})$, where $c \in \mathbb{Z}^+$ and κ is the cryptographic security parameter. This protocol only assumes a Common Random String.
  - Current best known protocol incurs $O(\kappa n^3)$ communication cost

Information-theoretic coin tossing protocol

- An information-theoretic one-shot asynchronous coin-tossing protocol with $n = 3t + 1$ and expected communication cost of $O(\kappa n^5)$. κ here is the statistical security parameter. This protocol can generate $O(n^2)$ common coins.
  - Current best known protocol incurs $O(\kappa n^6)$ communication cost for a single coin.

Reliable Broadcast (RBC)

- A balanced RBC protocol with good case latency of three-rounds and communication cost of $O(n|M|+\kappa n^2)$. Our protocol is not authenticated and takes five rounds in the worst case.
  - I do not know of any prior work on this problem.

Acknowledgements

I have many people to thank for many of these ideas. Zhuolun Xiang and my advisor Ling Ren has contributed to many of these ideas. Please contact me for details on contributors of any specific idea.