Ex4
due before the semester starts
version 1

Verifiable Secret Sharing and an Randomness Beacon

The goal of this question is to study Verifiable Secret Sharing (VSS) protocol and extend it to provide a simple (information theoretic) randomness beacon.

Your goal is to implement this functionality using $n = 5f + 1$ servers and withstand an adversary that can control f Byzantine servers in a synchronous model. You can assume communication can be done via secure and private point-to-point channels.

The ideal functionality of the Beacon has following interface:

- Each server can call *getRand*
- Once $f+1$ parties call *getRand* then the ideal functionality computes a uniformly random value r and sends r to all parties

In particular, the Beacon has the following properties:

- Liveness: if $f + 1$ honest parties call *getRand* then a value is returned after a constant number of rounds
- Correctness: all honest parties see the same value of the beacon
- Unpredictability: if no honest party calls *getRand*, then the adversary has no knowledge of the beacon value

1. Provide a protocol for the above functionality. Do not use any block box (if you need broadcast then implement it)
2. For unpredictability you may need to prove that the adversary value are binded before the beacon is revealed, explain why
3. For unpredictability you may need to prove that the adversary learns nothing before the beacon is revealed, explain why
4. Prove that your protocol has all the desired properties (implements the ideal functionality)