Recap of the Lectures on Secret Sharing

1 Secret Sharing Schemes

- Definition of a (t_c, t_s)-out-of-N secret sharing scheme
  - Share and Reconstruct algorithms
  - Correctness for sets of size at least t_c
  - Security for corrupted sets of size less than t_s (be able to prove security *and* to give concrete attacks if possible)
  - If $t_c = t_s$, we simply say t-out-of-N secret sharing
- Concrete secret sharing schemes
  - Additive secret sharing ($N = 2$, $N = 3$ and general case for any $N \in \mathbb{N}$)
  - Shamir secret sharing (and its packed version)
  - Replicated secret sharing
- Properties
  - Linearity
  - Multiplicativity

2 Pseudo-Random Generators and Functions

- Definition of a pseudo-random generator (PRG)
- Definition of a pseudo-random function (PRF)
- The GGM-tree to construct a PRF from a PRG (only the intuition required for the examen)

3 Pseudo-Random Secret Sharing

3.1 Sharing of Zero

- Definition of a (t_c, t_s)-out-of-N pseudo-random secret sharing scheme
  - Share and Reconstruct algorithms
  - Correctness for sets of size at least t_c, reconstructing to **the** 0 **value**
  - Security for corrupted sets of size less than t_s
  - If $t_c = t_s$, we simply say t-out-of-N secret sharing
- Concrete pseudorandom secret sharing schemes for sharings of zero
  - Graph with every party only two edges (Lecture 2)
  - Fully connected graphs (Lecture 3)
  - Over $\mathbb{Z}/2\mathbb{Z}$ with $\oplus$ (undirected graph)
  - Over $\mathbb{Z}/q\mathbb{Z}$ with $+$ and $-$ (directed graph)

3.2 Sharing of a Random Value

- Definition of a (t_c, t_s)-out-of-N pseudo-random secret sharing scheme
  - Share and Reconstruct algorithms
  - Correctness for sets of size at least t_c, reconstructing to a **pseudo-random value**
    Note: correctness definition contains a PPT adversary!
  - Security for corrupted sets of size less than t_s
  - If $t_c = t_s$, we simply say t-out-of-N secret sharing
- Concrete pseudorandom secret sharing schemes for sharings of random values
  - from replicated secret sharing