



General description

- ▷ Public key pk is a root hash c_*
- ▷ Secret key sk consists of all leafs x_{ij} .
- ▷ A signature σ is a minimal amount of information needed to recompute c_* .
- ▷ A secret key can be compressed by a pseudorandom function family.