1 Items

- Constructing Commitments, hiding vs binding.
- Review P, NP, IP.
- IP for Graph Non-Iso, amplifying soundness, correctness.
- Defining Zero-Knowledge
- ZK proof of Graph Non-Iso.
- ZK proof of all NP problems
- Sequential, parallel repetition of ZK proofs
- Constant round ZK
- Witness indistinguishability proof
- Non-Interactive proof systems
- Oblivious transfer construction
- Malicious security oblivious transfer
- Two party computation
- Yao's garbled circuit
- Defining multi-party computation
- Passively secure MP protocol
- Secret sharing
- Polynomial secret sharing, information-theoretic MPC.
- Extending to amlicious security, verifiable secret sharing
- Homomorphic encryption, EL Gamal, RSA
- Lattice
- Encryption using Lattice
- Fully-Homomorphic encryption