Constructions in CS127, Fall 2013

ASSUMPTIONS

RSA Assumption
Factoring Assumption
DDH Assumption
Discrete Log Assumption
“SHA-3 Assumption”
Quadratic Residuosity Assumption
Trapdoor Permutations
“AES Assumption”
One-Way Permutations
Collision-Resistant Hash Functions
One-Way Functions
P=NP

PRIMITIVES

Public-Key Encryption
Pseudorandom Functions
One-Way Functions
Pseudorandom Generators
Commitment Schemes
MACs
Fully Homomorphic Encryption
Homomorphic Encryption
Digital Signatures
Private-Key Encryption
ZK Proofs for NP

PROTOCOLS

Cloud Computing with Privacy
Private Information Retrieval
Secure Multiparty Computation
E-Voting
E-Cash
Secure Auctions
Private Datamining

Omitted: everything except P=NP implies one-way functions

= covered in class
= not covered, but known in literature