# Layer 3 – Interactive Protocols

**Standard commitment schemes** [EREZ]

1. Hash-based (random-oracle) commitments: define Commit(x) = HASH(x||r) where r is 128-bits random
2. Hash-based commitments: <http://cs.nyu.edu/courses/fall01/G22.3033-003/lect/lecture14.ps> , Section 2.3
3. Public-key encryption based commitments: commit to x by choosing new (pk,sk) and sending (pk,E(pk,x))
4. UC-secure commitment <http://eprint.iacr.org/2001/091>

**Trapdoor (equivocal) commitment schemes** [ERAN]

1. General transformation from Sigma protocol where simulator instructions are provided.

**Extractable commitment schemes** [ERAN]

1. Any commitment with a ZKPOK of committed value
2. Others?

**Homomorphic commitment schemes** [ERAN]

1. Take from LEGO: <http://eprint.iacr.org/2008/427.pdf>

**Sigma protocol** [HILA except for what is marked BENNY]

1. Sigma protocols for Damgard-Jurik [BENNY]
2. Sigma of committed value for Pedersen commitments [???]
3. Sigma of committed value for ElGamal commitments [???]
4. Sigma that committed value is as given - Pedersen [???]
5. Sigma that committed value is as given - El Gamal [???]
6. General compound statements [BENNY]

**Zero knowledge** [EREZ]

1. Fiat-Shamir transform for any Sigma protocol: just get verifier message by HASH(x,\alpha)

**Oblivious transfer** [HILA]

1. PVW\_UC (using any DH group or N-residuosity) [PVW], <http://www.cc.gatech.edu/~cpeikert/pubs/OTpaper.pdf>

**Oblivious polynomial evaluation** [BENNY]

1. Based on OT [BENNY]
2. Based on homomorphic encryption [BENNY]

**Information theoretic techniques** [GILAD] (take specification from VIFF)

1. Secret sharing (including general polynomial interpolation)
   1. Class that can work over any field
   2. Use Zp\* as basic field (here p can be small)
2. VSS
3. Arithmetic circuit protocols (addition, multiplication…)