Topics for the oral exam of cryptographic protocols
December 2008 – January 2009

1. “Classical” cryptographic protocols. Definitions of properties (confidentiality, authenticity), various attacks.
2. “Advanced” properties of cryptographic protocols. Denial-of-service, privacy.
3. Reconciling two views of cryptography.
4. Secret sharing, including verifiable secret sharing and decoding in the presence of wrong shares.
5. Goldreich-Micali-Widgerson method for secure two-party computation with semi-honest adversaries (a.k.a. The circuit evaluation algorithm at mpc1.pdf, right after Yao's garbled circuits). Includes definitional issues (in the semi-honest case).
6. Using secret sharing to implement MPC secure against semi-honest or malicious adversaries. Includes definitional issues. Does not include Rabin's and Ben-Or's protocol.
7. Universal composability. Definitions and composition theorem.
8. Universally composable cryptographic library. Real and ideal library and simulation.