Topics for the oral exam of cryptographic protocols
January 2011

1. “Classical” cryptographic protocols. Definitions of properties (confidentiality, authenticity). Various attacks and their classification. Dolev-Yao model. DoS-resilience. Privacy. Weak secrets.
2. Hybrid argument. Reconciling two views of cryptography.
3. Secret sharing, including verifiable secret sharing and decoding in the presence of wrong shares.
4. 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).
5. 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.
6. Universal composability. Definitions and composition theorem.
7. Universally composable cryptographic library. Real and ideal library and simulation.