

Lecture 11: Semantically Secure Public-Key Encryption I

*Instructor: Shafi Goldwasser**Scribes: Vahid Fazel-Rezai, Daniel Richman, Connor Sell***1 RSA preprocessing****2 Random Oracle Model Methodology****3 Types of Attacks**

- Lunchtime attack
- Timing attack
- Power attack
- Fault attack
- Cache attack

4 Public key crypto based on squaring**5 Nondeterministic public key crypto with trapdoor functions****6 Trapdoor predicates****7 Using single-bit encryption for arbitrary length encryption****8 Homomorphic encryption and some primitives****9 Probabilistic encryption scheme and examples****References**