Choose one of the papers below by the end of this week. You will read the paper completely, try to understand the contributions in detail and present the results to the class in a one hour presentation (end of October, beginning of November).

1- From Passive to Covert Security at Low Cost, Yehuda Lindell, Benny Pinkas, TCC 2011

2- Truly Efficient String Oblivious Transfer and SFE in Malicious and Covert Adversaries Models Using Resettable Tamper-Proof Tokens, Vladimir Kolesnikov, TCC 2010

3- Oblivious RAM Revisited, Benny Pinkas and Tzachy Reinman, CRYPTO 2010

4- Non-Interactive Verifiable Computing: Outsourcing Computation to Untrusted Workers, Rosario Gennaro, Craig Gentry and Bryan Parno, CRYPTO 2010

5- Improved Delegation of Computation using Fully Homomorphic Encryption, Kai-Min Chung, Yael Kalai and Salil Vadhan, CRYPTO 2010

6- Two-output Secure Computation With Malicious Adversaries. Abhi shelat and Chih-hao Shen, EUROCRYPT 2011

7- The IPS Compiler: Optimizations, Variants and Concrete Efficiency. Yehuda Lindell, Eli Oxman, and Benny Pinkas, CRYPTO 2011

8- Secure Computation on the Web: Computing without Simultaneous Interaction. Shai Halevi, Yehuda Lindell and Benny Pinkas, CRYPTO 2011