1. <http://xagawa.net/bib-lattice/?FHEs>.
2. You may present any paper from STOC, FOCS, Crypto, Eurocrypt, on any topic of cryptography, not necessarily on FHE. (Consult me if you want to present a paper from other conferences).
3. Preferred are papers on FHE, secure multiparty computation, computations on encrypted data.
4. One paper per lecture, by a team of three people.
5. Please email me the date, the paper you select, and the members of your team.
6. Please do not select Efficient Fully Homomorphic Encryption from (Standard) LWE (FOCS 2011, by Brakerski and Vaikuntanathan), which I am going to cover.

11/12, Tue, Daren Hrelic, Siyuan Ma, Zach Sjostrom

[Practical Techniques for Searches on Encrypted Data](http://www.cs.berkeley.edu/~dawnsong/papers/se.pdf) (2000) and newer results

11/14, Thu, Guoxing Chen, Liyuan Lei, Xi Yi

11/19, Tue, Fan Yang, Qiang Zhai, Wenjie Zhou

11/21, Thu, Sarah Al-Shareeda , Faisal Alanazi, Long Shi

11/26, Tue. Krieger, Ngo, Rossi

12/3, Tue, Barker, Can, Underwood