6.875 Spring 2017	**Project Proposal**
Skanda Koppula	
May 4, 2017	

The proposed two week project is first a literature overview of methods in literature to do practically efficient inference over encrypted data. The final project would be a roughly ten-page summary with the results of each unique work: formal cryptographic problem setup, the steps in the protocol algorithms and cryptosystem(s) employed, and the detailed proof of security.

Specifically, I had four papers in mind:

1. Machine Learning Classification over Encrypted Data (Goldwasser, et al.): `https://eprint.iacr.org/2014/331.pdf`
2. Crypto-Nets: Neural Networks over Encrypted Data (Naehrig, et al.): `https://arxiv.org/pdf/1412.6181.pdf`
3. Crypto-Nets (V2): High Throughput and Accuracy (Naehrig, et al.): `https://www.microsoft.com/en-us/research/wp-content/uploads/2016/04/CryptonetsTechReport.pdf`
4. Privacy Preserving Multi-party Machine Learning with Homomorphic Encryption (Ghasemi et al.): `https://pmpml.github.io/PMPML16/papers/PMPML16_paper_14.pdf`

Time permitting it would be interesting to, secondly, implement one method from these papers. I'm interested in the topic as it related to my current research work in fast biometric identification, and with biometric identification, privacy-preserving ways of doing this is good!