Meeting with Thang, 11/7/17

Meeting Notes composed by **Scott Russell**

Purpose:

- To discuss topics for Technology Research paper

Action Items after meeting:

- Change meeting time to **Tuesdays at 3 pm** (2 pm slots were all filled): awaiting approval from Thang

- Email Attila about **feedback for Requirements Document**.

- **Adjust Req. Document** based on said feedback. Resubmit and await approval.

- Start on personal segments **of Technology Review**.

Technology Review Key point

(provided by Andrew Ekstedt)

* Literature review: SSE algorithm (AE)
  + IM-DSSE
  + Cash
  + ...
* Crypto library (SM)
  + tomcrypt
  + OpenSSL
  + …
* Crypto primitive: PRF (AE)
  + AES
  + ChaCha20
  + …
* Crypto primitive: MAC (SM)
  + HMAC-SHA256
  + UMAC
  + Poly1305
* Cloud provider (AE)
  + dropbox
  + google drive
* Email protocol (SR)
  + POP3
  + IMAP
  + Exchange (MAPI)
* Programming Language (SM)
  + C++
  + Python
  + Cryptol?
* Experimental Design: benchmarking (SR)
  + how to compare with
    - IM-DSSE (C++ Bit Matrix)
    - Clusion (Java David Cash)
* Remote platform for running the server on (SR)
  + Amazon EC2
  + Google Compute
  + Microsoft Azure
  + flip

Parallelization: Not a major topic of discussion on its own but important due to time sensitive analysis.

- Using For loop keyword search.

- Send to separate threads for faster processing.

Literature Review:

As a project with aspects of research focus some aspects of the Technology review will be in the form of a Literature Review rather than using a typical Technology review template. Primary this will be for the SSE algorithm review.

Conclusion:

Continuing to work on design and preparation papers through capstone to get ready to start implementation. Direct implementation will most likely not start until the beginning of Winter term. The end of fall will be a time for feedback and zeroing in on key components of the project, how we will implement each piece, and options in the case of problems.