MQP Meeting minutes

Date and Time	Tuesday November 5th, 2013 at 2:00 pm
Venue	Craig's Office
Participants	Curtis, Craig, Krishna, Dan

Item	**Notes and Discussion**
Struggles with Python Bugs	• Current approach might not work very well • Client doesn't receive full response even though peers process it.
Goals for the Term	• Network testing with NS3 to figure out how memory and CPU intensive it is. • Consolidate the code base. • Streamline inter-party communication (perfect and implement the protocol, perhaps using HTTP). Right now the router to router communication could be more organized. • Build a trust model that peers can use when selecting neighbors for an aggregation session. Look to P2P for inspiration, as their protocol is built on trust (many ways to go about this, what's right for P2P might not be good for us).
Trust Model	• Verification of data: buffer full response and check at the end. • What happens when a peer sends back untruthful data? Dock their score or drop them completely. • What if the web server lies to a peer? Breaks current verification model. • Literature review of how P2P networks do this, and design the protocol in a manner similar to this. Cite'em! • An hour in the library is worth a week in the lab.
Security	• Figure out what cryptographic protocols and libraries to use for signing each initial request (to tie responsibility to peers). Python libraries likely exist, find them. • Encryption/MACing/Asymetric Signing primitives, find which to use.
Misc	• Testing: Poke around with NS3, Routers and VMs. • What does this protocol look like to the server? Will our range retrieval approach become a problem for servers that only allow one download per client. What if the server figures out the Dan protocol and poisons the zero knowledge proof answers. • Write about everything. (3 pages per week as an arbitrary minimum)