MQP Meeting minutes

Date and Time	Tuesday 10 December 2013 at 2:00 pm
Venue	Craig's Office
Participants	Curtis, Craig, Krishna, Dan

Item	Notes and Discussion
Pycrypto and Repudiation	• Set up message signing and signature verification between clients. • Inputs = target url. This is not enough to guarantee good repudiation.
Breaking the Repudiation System	• Hash(url + timestamp) and sign it. If a router tries to spoof the request after the original signature is signed, the verification will always fail. • Temporality of access is extremely important. We want to keep the timestamp associated with each request in our logs. • How do we combat private keys that "go public" (and are therefore compromised)?
Emulating a notary	• Two way handshake? Sign original request on receiver end and send back, which is resigned finally. "A notary" • Both keys would have to leak to violate non-repudiation. • Handshake with a centralized server? - decentralized more simple in our case. • Farm out to other peers. They verify the signature and add timestap, and sign it themselves, who returns it to the original worker. • Have the entire network verify the request at once? What is the cost of a large scale notarization. Add to discussion.
Next Week	• Checkpoint on writing and code deliverable • Discussion on repudiation again