**Thesis:** On the Cryptographic Deniability of the Signal Protocol

**Abstract:** Offline deniability is the ability to a posteriori deny having participated in a particular communication session. This property has been widely assumed for the Signal messaging application, yet no formal proof has appeared in the literature. In this study, we present the first formal study of the offline deniability of the Signal protocol. Our analysis shows that building a deniability proof for Signal is non-trivial and requires strong assumptions on the underlying mathematical groups where the protocol is run.

To do so, we study various implicitly authenticated key exchange protocols including MQV, HMQV and 3DH/X3DH, the latter being the core key agreement protocol in Signal. We first present examples of mathematical groups where running MQV results in a provably non-deniable interaction. While the concrete attack applies only to MQV, it also exemplifies the problems in attempting to prove the deniability of other implicitly authenticated protocols, such as 3DH. In particular, it shows that the intuition that the minimal transcript produced by these protocols suffices for ensuring deniability does not hold. We then provide a characterization of the groups where deniability holds, defined in terms of a knowledge assumption that extends the Knowledge of Exponent Assumption (KEA).

We conclude by showing two additional positive results. The first is a general theorem that links the deniability of a communication session to the deniability of the key agreement protocol starting the session. This allows us to extend our results on the deniability of 3DH/X3DH to the entire Signal communication session.

**Committee:**

- Professor Rosario Gennaro, Mentor, The City College
- Professor Nelly Fazio, The City College
- Professor William E. Skeith, The City College

**Outside member:**

- Dr. Hugo Krawczyk, Outside Member, Algorand Foundation