Abstract: Although offline deniability (the ability to a posteriori deny having participated in a particular communication session) has been widely claimed for the Signal messaging application, no formal proof has ever appeared in the literature. In this study we discuss the reasons why a meaningful deniability proof may be difficult to construct.

To do so we discuss various implicitly authenticated key exchange protocols such as MQV, HMQV, 3DH and X3DH, the latter being the core key agreement protocol in Signal. We are able to present examples of mathematical groups where running MQV results in a provably non-deniable interaction. This MQV counter-example exemplifies the problems one encounters in trying to prove the deniability of all the other implicitly authenticated protocols, such as 3DH. We provide a characterization of the groups where deniability holds by essentially assuming that the equivalent characterization of non-deniability is not met. However, using this assumption does not give us much information about whether deniability actually holds true in practice or not.

We conclude by showing two 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. Additionally we show that very simple modifications to the implicitly authenticated key exchange protocols listed above (including 3DH) would yield provable deniability, and therefore would be a more suitable choice for the underlying key agreement step of Signal and other off-the-record messaging applications.

Committee:

- Professor Rosario Gennaro, mentor, The City College of New York
- Professor Nelly Fazio, The City College of New York
- Professor William Skeith, The City College of New York

Outside Member:

- Professor Hugo Krawczyk, Algorand Inc