**Getting back to TLS….**

I think I have been getting ahead of myself. We first need to get basic TLS1.3 working as per the RFC8446. As I see it KEM-TLS and IBE-TLS will be developed later as experimental forks of the main project.

(I was thinking that drones would make a nice IoT testbed for experimentation... Its important that drone to ground station communications are fully encrypted, and an IBE-TLS protocol with a fully encrypted handshake might be a nice fit...)

**Alerts**

The word Alert appears 144 times in the RFC. It is an important part of the implementation that the correct alert is sent under each of the myriad of alert conditions that can arise, and that the protocol is cleanly terminated. Its relatively simple to get TLS1.3 working on the assumption that all will go well, but a full implementation must be prepared for failure, and must give the correct response as defined in the RFC. Note that in TLS1.3 all alerts are fatal – except “close notify” (which simplifies things a little).

Alerts can be sent by either the client or the server. So I have prepared two spreadsheets where we can record our status. Basically the spreadsheet records the condition under which an alert should be sent, which alert is sent, and whether or not it is currently implemented. Note that in addition to these alerts, others (like Certificate Expired) are not specifically mentioned in the RFC, other than noted in section 6.2

Furthermore all of these alert conditions must be simulated to ensure proper implementation. Lots to do!