Fahad's results for thesis

Part 1 (regular expressions)

- he corrected the paper by Sulzmann and Lu by giving a new definition for POSIX matching—his proof is completely different than the one by Sulzmann and Lu and formalised in Isabelle
- he extended the results by Sulzmann and Lu to all regular expression constructors, excluding back references; to deal with backreferences is probably too difficult for the remaining time
- he formalised in Isabelle the definition of POSIX matching by Okui and Suzuki and showed that it is equivalent to his definition (his definition is declarative, whereas the one by Okui & Suzuki is by a position caluculus—so both definitions are quite different technically, but the result is that they define the same 'thing')
- from his correctness result for the algorithm by Sulzmann and Lu, he proved the correctness of various stages of optimisations: POSIX matching including simplification of regular expressions; bit-coded representation of regular expressions has not yet been done, but should be easy to do in the remaining time

Part 2 (TLS protocol in F-Star/internship at Microsoft Research in Cambridge)

- he added features to the F-Star language in order to verify their TLS parser in F-Star
- he created a verified byte-library for F-Star, which provides an API to manipulate byte sequences and indexed arrays
- he modified the existing TLS parser in F-Star to use his new byte library for the representation of strings
- verification of the parser is not yet done, but the hope is he finishes this by the end of his internship (in Sepember)