Exercise 7.1 (Project, part 3). (10+10 points)

Consider your chosen protocol for this exercise.

(i) Discuss the security of the chosen protocol under the same security aspects as we did for TLS:

- Session key agreement.
- Perfect forward security.
- Denial of Service.
- Endpoint identifier hiding.
- Live partner reassurance.

(ii) Which security results do exist for your chosen protocol? +10

Have a look at the most promising one.

- Is the entire protocol considered?
- Is an automated proof considered/described?
- Are concrete bounds given or only asymptotical?
- Which proof model is used: computational standard model (via game-hopping) as in the course or a different one?

We will summarize your results in course and tutorial soon.