Week 1

Started on the project. Lluis sent me some research papers to read on.

Week 2

Discussed paper on privacy amplification. I started to read on Shannon Theory and density matrix.

Week 3

Discussed Shannon Theory, which helped me to understand the project.

Started reading on cloning machines and started drafting project plan.

Week 4

Questions

1. Should I do literature survey now or when I write the report? **Can write literature survey and background now, but leave the actual work part until finishing the research.**
2. Finalising project plan (objectives, deliverables) **done**
3. Get a start on solving the problem **lluis gave some hints**
4. Should I write the main part of the report in the form of research papers? **Yes, similar to the papers I read. Emphasising on present my findings, how I conducted the research, avoid explaining the maths behind my findings in detail.**
5. How should I schedule the project timeline? **Work on the opt problem for now**
   1. Preliminary work (til end of Oct)
   2. Solving the problem (analysing, modelling) (Nov to mid Jan)
   3. Evaluation and testing (mid Jan to mid Feb)
   4. Writing report (mid Feb til April) **milestones to be added**

Meeting:

1. Lluis reviewed project plan. I submitted project plan.
2. Start to work to deriving the key generating function as theta and error rate.

Week 5 – 7

Derived R as a function of phi and error rate.

Worked out optimal phi for each error rate.

Analysis and plots.

Week 8

Started to work on the alternative B92 protocol with 3 states instead of 2.

Week 9

B92 with 3 states does not work.

Start to investigate:

1. Individual attack
2. Optimal attack for B92.

Week 10

Present individual attack, and collective vs individual attack comparison.

Week 11

Submit interim report. Draft bullet points for results and algorithm section.