1 burning questions

-

2 current todo's

- change to ind-$
- in meer detail opschrijven wat de variables zijn van de sec games en wat de aannamens zijn
- beginnen met schrijven in main

3 main idea

The PKC paper ends with a ADEM + AMAC construction as "solution". The original paper from ENC -¿ MAC has been revised, so this should prob be revised as well. In general its nice to write down thing in a more "sym crypto" style as we use symmetric primitives. It would probably also be nice to revise it more in general and see what other ways there are to reach the end-goal expected in the PKC paper.