1 Papers referred to

1. Marie-Sarah Lacharite, Kenneth G. Paterson. **Frequency-smoothing encryption: preventing snapshot attacks on encrypted databases**

2. Thomas Baign‘eres, Pascal Junod, and Serge Vaudenay. **How Far Can We Go Beyond Linear Cryptanalysis?**

2 FSE revisited

- The security model measures the advantage of the adversary differentiating the resulting distribution from uniform distribution but the KL divergence used is an approximation to some other value (P_e) in the second paper listed above.

- The encryption scheme does not consider correlation between columns, i.e. encryption is done column by column.

- Maybe correlation can be exploited to attack the scheme. (**See folder ‘Attack on FSE’**)

3 More on formalising the frequency smoothing problem

- Cutting and padding are operations which will cause expansion of data size. We need to define a cost function to measure the performance of our frequency smoothing algorithm.

- We need to define security more carefully: we may not need uniformly distributed histogram by the end, e.g. a histogram that has two levels and attributes are randomly assigned to each one of them.