1 Papers referred to

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

2 Formalising the frequency smoothing problem

- We consider the static case, i.e. we are given the realization of the database (not a distribution) and try to hide frequencies of the attributes,
- The main techniques identified are cutting (reducing height of the high-frequent attributes) and padding.
- Correlation between columns need to be considered too.

3 A new OPE scheme

- Modified the construction so that the claim made in the earlier meeting is indeed met. **Modification:** instead of only merging disjoint blocks at each level, the 'sliding window' only moves by one block at each time. The time/space complexity stays the same because the modification only results in an expansion factor of space by 2.
- Security of this scheme is not analysed yet. (**To think:** is security with a simulator proof (even perfectly defined) sufficient to ensure security in practice?)

4 A weaker OPE scheme

- **Idea:** instead of having all the blocks to answer queries, we use only the bottom layer.
- In that case, relative order of the blocks will be revealed with queries. But how do we quantify leakage in this case?