1 Papers referred to

1. Marie-Sarah Lacharite, Brice Minaud. **Improved Reconstruction Attacks on Encrypted Data Using Range Query Leakage**
2. **K-Nearest-Neighbour Search on Encrypted Data** (Not published yet)
3. Rafail Ostrovsky. **Software Protection and Simulation on Oblivious RAMs**
4. Data structure and algorithms I have learnt during undergraduate.

2 A new OPE scheme

- The idea is to use 'searchable' data structures to pre-process the queries so that the queries do not leak the sets used in 1.
- TBD: include the images describing the scheme.
- To think: what does the scheme leak?

3 ORAM

- Confirms that the lower-bound of overhead is indeed $\mathcal{O}(\log n)$.
- Question to be answered: is ORAM any similar to OPE in the sense that, in order to hide access pattern, how much overhead does it cost?

4 Syntax of encrypted database

- We can think of database in three levels: a string of zeros and ones in the most abstract form, a database as a set of strings, and a database with all the details.
- We will formalize syntax on the most abstract form first.
- Notation (need better names):
  - **Initialise**: $1^\lambda \rightarrow \text{params}^*$
  - **KeyGen**: $1^\lambda \rightarrow \mathbf{sk}$
  - **Enc**: $1^\lambda \times \mathbf{sk} \times \mathbf{DB} \rightarrow \mathbf{EDB}$
  - **Dec**: $1^\lambda \times \mathbf{sk} \times \mathbf{EDB} \rightarrow \mathbf{DB}$
  - **Q**: $\mathbf{DB} \times Q \rightarrow \mathbf{DB}$
  - **encQ**: $1^\lambda \times \mathbf{sk} \times Q \rightarrow \mathbf{eQ} \times \mathbf{iQ}$
  - **EQ**: $1^\lambda \times \mathbf{sk} \times \mathbf{EDB} \times \mathbf{eQ} \rightarrow \mathbf{EDB}$
  - **DQ**: $1^\lambda \times \mathbf{sk} \times \mathbf{EDB} \times \mathbf{iQ} \rightarrow \mathbf{DB}$