1 Attack against Searchable Encryption

In the setting of searchable encryption, documents are attached with a set of keywords each, and the goal of searchable encryption is to produce some secure data structure so that the user can query (encrypted) keywords, and the server returns the list of documents contains that keyword.

1.1 IKK Attack

- In paper: Access Pattern disclosure on Searchable Encryption: Ramification, Attack and Mitigation.
- URL: `http://www.utdallas.edu/~mxk055100/publications/ndss2012.pdf`.
- Authors: Mohammad Saiful Islam, Mehmet Kuzu, Murat Kantarcioglu.
- Attack requirement: prior distribution on the co-occurrence matrix.
- Attack method: use simulated annealing (a heuristic optimisation technique) to find a permutation between keywords and trapdoors. It can also be seen as minimisation of distance between prior distribution and realization (with rows and columns randomly permuted) of co-occurrence matrices.

1.2 Count Attack

- In paper: Leakage-Abuse Attacks Against Searchable Encryption.
- Authors: David Cash, Paul Grubbs, Jason Perry, Thomas Ristenpart.
- URL: `https://eprint.iacr.org/2016/718.pdf`.
- Attack requirement: exact counts in co-occurrence matrix.
- Attack method: find matches between counts in co-occurrence matrix and number of documents returned by queries.

- **Note to myself:** We probably need much less information than the full co-occurrence matrix to recover keywords, because the way co-occurrence matrix is constrained: knowing one keyword means knowing one row up to permutation. It is interesting to see if we can construct an attack that requires way less information than that in the paper ($|W|^2$ entries in the co-occurrence matrix).

1.3 Graph Matching based Attack

- In paper: The Shadow Nemesis: Inference Attacks on Efficiently Deployable, Efficiently Searchable Encryption.
- URL: `https://pdfs.semanticscholar.org/a344/060ddde7b86e8f2105ed8b96a54954e pdf`.
- Authors: David Pouliot and Charles V. Wright.
- Attack requirement: prior distribution on the co-occurrence matrix.
- Attack method: view the co-occurrence matrix as an instance of graph matching problem and apply approximation algorithms that solves it.

2 Attack against Property-preserving Encrypted Databases

2.1 Inference Attack

- In paper: Inference Attacks on Property-Preserving Encrypted Databases.
- Authors: Muhammad Naveed, Seny Kamara, Charles V. Wright.
- URL: `https://cs.brown.edu/~seny/pubs/edb.pdf`.
- Attack requirement: prior knowledge on plaintext distribution.
- Underlying PPE: DE and OPE

- Attack method: Match prior distribution to realization. Only use single-column distributions.

2.2 Reconstruction Attacks using Access Pattern on OPE/ORE

- In Paper: Generic Attacks on Secure Outsourced Databases
- Authors: Georgios Kellaris, George Kollios, Kobbi Nissim.
- URL: `https://privacytools.seas.harvard.edu/files/privacytools/files/generic.pdf`.
- In paper: Improved Reconstruction Attacks on Encrypted Data Using Range Query Leakage.
- Authors: Marie-Sarah Lacharité, Brice Minaud.
- `https://eprint.iacr.org/2017/701.pdf`.
- Attack requirement: access to enough queries ($\mathcal{O}(N^4)$ in the first paper and $\mathcal{O}(N^2)$ in the second, they differ from each other because the assumption on query distributions are different, but the attacks are the same).
- Underlying PPE: OPE.
- Attack method: Abuse order-preserving property in the results of queries. e.g. if $x_0 < x_1 < x_2$, and we write $Q(x, y)$ to denote query result (as a set). Then by knowing $Q(x_0, x_1)$ and $Q(x_0, x_2)$, we also know $Q(x_1, x_2)$. Hence it is possible to recover query results for singletons (query on single plaintext rather than a range) completely, up to reflection.

2.3 Paper to read

- In paper: Leakage-Abuse Attacks against Order-Revealing Encryption.
- Authors: Paul Grubbs, Kevin Sekniqi, Vincent Bindschaedler, Muhammad Naveed, Thomas Ristenpart.

- URL: `https://eprint.iacr.org/2016/895.pdf`.
- Note: This paper cites a few other papers with attacks with high recovery rate, worth to read all of them. We will see if our proposed scheme is secure under these attacks.

3 Other attacks

3.1 Variance Attack

- Underlying PPE: DE.
- Attack requirement: prior knowledge on plaintext distribution.
- Attack method: For random variables X, Y, $\mathbb{E}(X) = \mathbb{E}(y)$ is not sufficient to make the random variables indistinguishable. Given a realization, we know if the observed value is more likely to come from X or Y.

3.2 Co-occurrence attack on FSE

- Underlying PPE: FSE.
- Attack requirement: prior knowledge on plaintext distribution.
- Attack method: Similar to count attack in principle, but with additional technique to handle randomness in observed values.

4 Various Other Attacks

There are many other attacks including file injection attack and query volume attack. They are either trivial or active, so we will not discuss them here (or just yet).