1 Papers referred to

1. Benjamin Fuller, Mayank Varia, Arkady Yerukhimovich, Emily Shen, Ariel Hamlin, Vijay Gadepally, Richard Shay, John Darby Mitchell, Robert K. Cunningham. **SoK: Cryptographically Protected Database Search**
2. David Cash, Paul Grubbs, Jason Perry, Thomas Ristenpart. **Leakage-Abuse Attacks Against Searchable Encryption**
3. Kellaris G, Kollios G, Nissim K, O'Neill A. **Generic Attacks on Secure Outsourced Databases**
4. Xiao Shaun Wang, Kartik Nayak, Chang Liu, T-H. Hubert Chan, Elaine Shi, Emil Stefanov, Yan Huang. **Oblivious Data Structures**
5. Emil Stefanov, Marten van Dijk, Elaine Shi, T-H. Hubert Chan, Christopher Fletcher, Ling Ren, Xiangyao Yu, Srinivas Devadas. **Path ORAM: An Extremely Simple Oblivious RAM Protocol**
6. Marie-Sarah Lacharite, Brice Minaud. **Improved Reconstruction Attacks on Encrypted Data Using Range Query Leakage** (have not read the paper yet but have a rough idea what it is about)
7. A few more papers cited in 1, 2 and 4
8. Related lectures from `https://www.youtube.com/playlist?list=PLXF_IJaFk-9ADeshgHXrSfuwPyEMa5qS7`

2 Overview of literature in encrypted searchable databases

- See 1.1. There are three broad types of encrypted searchable databases: legacy, custom inverted index, and custom tree traversal. All of which leaks access pattern.
- Oblivious approaches does not leak access pattern but the bandwidth blowup is lower-bounded by $\mathcal{O}(\log(n))$.
- Although documents are encrypted using randomized encryption schemes most of the times, the view of the server is a deterministic copy. So file retrieval reveals the query itself. That also means randomized padding based schemes will not work on OPE, due to 6.

3 ORAM

- ORAM is a potential solution to the encrypted searchable databases problem, but its time complexity is not desirable.
- Remain to revisit the paper that proves the lower-bound on bandwidth blowup.

4 Attack against OPE

- Counting attack in 2 is already sufficient to recover the entire database given prior distribution.
- 6 provides a more time-efficient solution and can work without prior information.
- Have to read the paper before next meeting.