Mitigating Attacks on Encrypted Databases via Adjustable Leakage

Ioannis Demertzis, University of Maryland

Searchable encryption (SE) allows a client to outsource a dataset to an untrusted server while enabling the server to answer various queries, such as point queries or range queries, in a private manner. SE schemes have proven to be very practical at the expense of well-defined leakage such as search and access pattern. Nevertheless, a plethora of attacks in the literature utilize these leakages to recover the dataset or the search queries. Defenses against such leakage-abuse attacks typically require the use of Oblivious RAM or padding the query result with a large number of dummy entries---such countermeasures are however quite impractical.

In order to efficiently defend against such leakage-abuse attacks, we propose new SE schemes with adjustable leakage. That is, the amount of privacy loss expressed in leaked bits of search or access patterns can be defined at setup. This allows us to effectively defend against leakage-abuse attacks, without sacrificing performance: As our experiments show, when our constructions protect only few bits of the above leakages, is enough for most of the attacks to fail, while the performance of our schemes are close to traditional (non-adjustable) SE.