Cryptology ePrint Archive: Report 2013/086

Efficient Private File Retrieval by Combining ORAM and PIR

Travis Mayberry and Erik-Oliver Blass and Agnes Chan

Abstract: Recent research results on "bucketed" Oblivious RAM by Shi et al. [12] reduce communication for an N-capacity storage with blocks of size l bits to poly-logarithmic complexity O(l · log^3(N)) in the worst- case. The individual buckets, however, are constructed using traditional ORAMs which have worst-case communication complexity being linear in their size. PIR protocols are able to provide better worst-case bounds, but have traditionally been less practical than ORAM due to the fact that they require O(N) computation complexity on the server. This paper presents Path-PIR, a hybrid ORAM construction, using techniques from PIR, that overcomes the individual weaknesses of each. Path-PIR's main idea is to replace the individual buckets in the ORAM construction by Shi et al. [12] with buckets backed by PIR. We show that this leads to orders of magnitude smaller data transfer costs for practically sized databases, compared to existing work, and achieves better asymptotic communication O(l · log^2 (N)) for large block sizes. Additionally, the typically high computational cost of PIR is negated by the small size of the individual buckets. We also show that Path-PIR has very low latency, i.e., a low amount of data is required before a user receives the result of his data request (approximately 4 times the block size). Using Amazon EC2, we demonstrate that monetary cost induced by the server's PIR computation are far outweighed by the savings in data transfer.

Category / Keywords: cryptographic protocols / private information retrieval, oblivious ram

Date: received 19 Feb 2013, last revised 10 Apr 2013

Contact author: travism at ccs neu edu