PanORAMa: Oblivious RAM with Logarithmic Overhead

Mariana Raykova, Google

We present PanORAMa, the first Oblivious RAM construction that achieves communication overhead $O(\log N \cdot \log \log N)$ for database of N blocks and for any block size $B = \Omega(\log N)$ while requiring client memory of only a constant number of memory blocks. Our scheme can be instantiated in the ""balls and bins"" model in which Goldreich and Ostrovsky [JACM 96] showed an $\Omega(\log N)$ lower bound for ORAM communication.

Our construction follows the hierarchical approach to ORAM design and relies on two main building blocks of independent interest: a new oblivious hash table construction with improved amortized $O(\log N + \text{poly}(\log \log \lambda))$ communication overhead for security parameter λ and $N = \text{poly}(\lambda)$, assuming its input is randomly shuffled; and a complementary new oblivious random multi-array shuffle construction, which shuffles N blocks of data with communication $O(N \log \log \lambda + N \log N / \log \lambda)$ when the input has a certain level of entropy. We combine these two primitives to improve the shuffle time in our hierarchical ORAM construction by avoiding heavy oblivious shuffles and leveraging entropy remaining in the merged levels from previous shuffles. As a result, the amortized shuffle cost is asymptotically the same as the lookup complexity in our construction.

Joint work with Sarvar Patel, Giuseppe Persiano, Kevin Yeo