Leakage in the Cell Probe Model: Lower Bounds for Response Hiding Encrypted Multi-Maps.

Giuseppe Persiano, U. Salerno

The cell probe model has been recently used to give lower bounds on the efficiency of cryptographic construction such as ORAM. In this talk we extend the cell probe model to consider leakage and study the efficiency of encrypted multi-maps, a primitive that has been used to construct searchable encryption schemes.

We present negative results showing that {\em dynamic on-line response-hiding} constructions for encrypted multi-maps have efficiency lower bounds of $\Omega(\log n)$.

The lower bound is tight as we describe a simple dynamic construction that matches the lower bound with optimal $O(\log n)$ efficiency and small leakage consisting of only query response lengths and inserted document sizes.

Finally, we present hardness results showing that lower bounds for either {\em offline} or {\em static} response-hiding schemes would imply lower bounds for sorting circuits and/or locally decodable codes.

Joint work with Sarvar Patel and Kevin Yeo.