

Tomáš Masařík  
masarik@kam.mff.cuni.cz

Presented paper by Zeev Dvir, Sivakanth Gopi  

2–server PIR with sub-polynomial communication

Definitions

**Definition** PIR A $k$–server Private Information Retrieval (PIR) is triplet of algorithms: $(Q, A, R)$.

- At the beginning user obtains a random string $r$, $i$ position of bit and invokes queries $q_1, \ldots, q_k$ using algorithm $(q_1, \ldots, q_k) = Q(i, r)$.
- Then sends $q_j$ to $j$th server (with database $D$) which responds with an answer $a_j$ using algorithm $a_j = A(j, D, q_j)$.
- Finally, user computes value of $i$th bit of the database $D$ using algorithm $D_i = R(a_1, \ldots, a_k, i, r)$.

The important thing is privacy: each server learns no information about $i$. For any fixed server $j$ the distribution over random strings $r$ of $q_j = (i, r)$ is identical for every $i$.

The communication cost of that protocol is worst case number of bits exchanged between the user and the servers.

**Theorem** [Main result] There exists a 2–server PIR with communication cost $n^{o(1)}$.

**Definition** [Matching vector family] $S$–Matching vector family is a pair $(U, V)$ of $n$-tuples, each of them is a $k$ dimensional vector.

Such that $< u_i, u_j > = 0$ iff $i = j$ and $< u_i, u_j > \in S$ iff $i \neq j$.

**Theorem** [Matching vector family construction (Grolmusz 99)] There is an explicit constructible $S$–matching vector family in $Z_k^n$ of size $n \geq \exp(\Omega((\log k)^2))$ with $S = \{1, 3, 4\}$