Universidade de Aveiro
2017-2018

Nearest private query based on quantum oblivious key distribution

Mariana Ferreira Ramos
(marianaferreiraramos@ua.pt)

Department of Electronics, Telecommunications and Informatics,
University of Aveiro, Aveiro, Portugal
Instituto de Telecomunicações, Aveiro, Portugal

Nearest private query based on quantum oblivious key distribution

- Nearest private query (**NPQ**) involves two parties, a user (Alice) and a data owner (Bob).

  Alice has a secret input, x, and Bob has a private data set $B = \{x_1, x_2, ..., x_m\}$, where $x_i \varepsilon \{0, 1, ..., N-1\}$ and $1 \leq i \leq m$, and $N = 2^n$.

- Alice wants to know which element x_i in Bob's private data set (**B**) is the closest to x without revealing it.

- Bob cannot learn any secret information about the secret x (**Alice privacy**).

- Alice cannot know any other secret information about the private data set B except the nearest to x_i (**Bob privacy**).

- They use a QOKD which is the base of the quantum protocol for nearest private query.

NPQ protocol

Lets assume,

- Alice secrete parameter $x = 8$.
- Bob private data set $B = \{1, 2, 3, 6, 7, 10, 11, 14\}$, being $m = 8$, $n = 4$ and $N = 16$.

Step 1 Bob generates a 16-element data set $D = \{D(0), ..., D(15)\}$ where $D(j) = x_l$, being x_l the closest element to **j** in Bob data set **B**.

NPQ protocol

j	D(j)	
0	1	0 0 0 1
1	1	0 0 0 1
2	2	0 0 1 0
3	3	0 0 1 1
4	3	0 0 1 1
5	6	0 1 1 0
6	6	0 1 1 0
7	7	0 1 1 1
8	7	0 1 1 1
9	10	1 0 1 0
10	10	1 0 1 0
11	11	1 0 1 1
12	11	1 0 1 1
13	14	1 1 1 0
14	14	1 1 1 0
15	14	1 1 1 0

QOKD procedure

Bob and Alice will apply QOKD procedure n times in order to establish n keys.

- Bob keys are denoted as $K_1, K_2, \ldots, K_n$ and he knows all bits of each K_i.
- Alice keys are denoted as $K_1^*, K_2^*, \ldots, K_n^*$, but she only knows $K_i(x)^*$ (xth bit of the key K_i^*).

Lets describe how the first key is generated. The following keys are generated in the same way.

1 - Bob prepares a long set of encoded photons (18) with $a = 3$. a represents the maximum number of bits that Alice should know. Bob sends the photons one by one to Alice.

2 - Alice measures the photons in a random basis and announces with measurements she performed successfully.

QOKD procedure

3 - For each photon that Alice measured successfully Bob announces 1 or 0, depending on the original state of the photon.

4 - Based on her measurements and Bob's declaration, Alice can obtain the sent bit with certain probability.

Alice and Bob share a raw key string with length $N + a - 1$ equals to 18 in this case.

- Bob fully knows all bits,

$$ROK_B = 001001110001110101.$$

- Alice only knows a quarter of bits theoretically,

$$ROK_A = 0?????110????????1.$$

QOKD procedure

In order to control the number of bits known by Alice in the final oblivious key FOK_A Bob calculates the security parameter k which is equal to 2 in this case, and then the obtain:

$$FOK_B = 0110100100100111 11$$

$$FOK_A = ??????01??????????1.$$

Now, from a bits known, Alice randomly chooses $a-1$ bits to check Bob's honesty by requesting him to announce this bit values. If these bits are the same recorded by Alice she knows he is being honest. Otherwise, she stops the protocol.

Lets assume Bob is honest, this way Bob discarded the checked $a-1$ bits from their FOKs.

QOKD procedure

At this time, they have:

$$FCOK_B = 0110100001001111$$

$$FCOK_A = ??????0?????????.$$

Then, according to Alice private parameter, $x = 8$ and known bit position in $FCOK_A$ in at position $y = 6$, Alice gets $s = y - x = -2$ and sends it to Bob. Now, they right shift the respective FCOKs 2 bits and obtain the first key

$$K_1 = 1101101000010011$$

$$K_1^* = ???????0???????.$$

They repeat this procedure 4 times to found the four keys.

QOKD procedure

j	D(j)		K_1	K_2	K_3	K_4	K_1^*	K_2^*	K_3^*	K_4^*
0	1	0 0 0 1	1	1	1	0	?	?	?	?
1	1	0 0 0 1	1	0	1	1	?	?	?	?
2	2	0 0 1 0	0	0	0	1	?	?	?	?
3	3	0 0 1 1	1	1	0	0	?	?	?	?
4	3	0 0 1 1	1	1	1	0	?	?	?	?
5	6	0 1 1 0	0	0	1	0	?	?	?	?
6	6	0 1 1 0	1	0	0	1	?	?	?	?
7	7	0 1 1 1	0	0	1	1	?	?	?	?
8	7	0 1 1 1	0	1	1	0	0	1	1	0
9	10	1 0 1 0	0	1	1	1	?	?	?	?
10	10	1 0 1 0	0	0	0	1	?	?	?	?
11	11	1 0 1 1	1	0	1	1	?	?	?	?
12	11	1 0 1 1	0	0	1	1	?	?	?	?
13	14	1 1 1 0	0	1	0	0	?	?	?	?
14	14	1 1 1 0	1	0	0	0	?	?	?	?
15	14	1 1 1 0	1	0	1	0	?	?	?	?

NPQ Protocol

At this time Bob is able to encode all numbers with correspondent keys but Alice only will cable of decode position 8.

Alice rightly gets the query result x_5 in Bob's data set, i.e 7, which is the closest result to x in the private data set B.

E-mail: marianaferreiraramos@ua.pt