Universidade de Aveiro
2017-2018

Quantum Oblivious Key Distribution with Discrete Variables

Mariana Ferreira Ramos
(marianaferreiraramos@ua.pt)

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

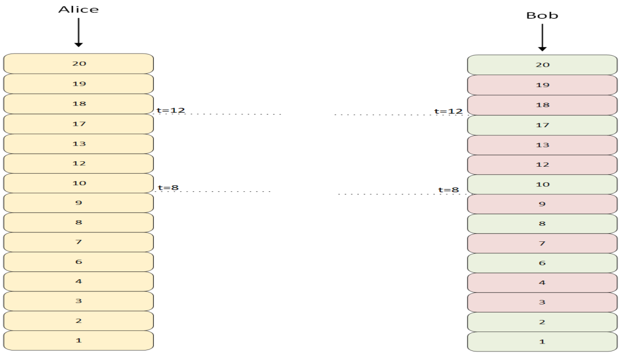
INSTITUIÇÕES ASSOCIADAS:

instituto de telecomunicações

creating and sharing knowledge for telecommunications

Quantum Oblivious Key Distribution System (QOKD)

The QOKD system enables two parties (Alice and Bob) to share a set of keys. These keys have the particularity of being half right and half ~~wrong~~. Only Bob knows which are right and ~~wrong~~ bits. Alice only knows that at some tabs there are the same number of right and ~~wrong measurements~~.



~~This can be used for guarantee security in communication protocols between two parties.~~

Oblivious Transfer

- Alice has two messages m_0 and m_1 and Bob wants to know one of them, m_b, without Alice knowing which one, i.e. without Alice knowing b, and Alice wants to keep the other message private, i.e. without Bob knowing $m_{\bar{b}}$. Lets assume $m_0 = \{0011\}$ and $m_1 = \{0001\}$.
- Bob defines two sub-sets with size $s = 4$:

$$I_w = \{3,4,7,9\},$$

and

$$I_r = \{1,2,6,8\},$$

where I_w is the sequence of positions in which Bob was wrong about basis measurement and I_r is the sequence of positions in which Bob was right about basis measurement.

Oblivious Transfer

- Alice defines two encryption keys K_0 and K_1 using the values in positions defined by Bob in the set sent by him. Lets assume,

  $$K_0 = \{1, 1, 1, 0\}$$

  $$K_1 = \{0, 0, 0, 1\}.$$

  Alice does the following operations:

  $$m = \{m_0 \oplus K_0, m_1 \oplus K_1\}.$$

- Alice sends to Bob through a classical channel

  $$m = \{1, 1, 0, 1, 0, 0, 0, 0\}.$$

Oblivious Transfer

- Bob uses S_{B1}, values of positions given by I_r and I_w and does the decrypted operation.

$$
\begin{array}{c|cccccccc}
m & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
\hline
\oplus & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0
\end{array}
$$

The first four bits corresponds to message 0 and he received $\{0,0,1,1\}$, which is the right message m_0 and $\{0,1,1,0\}$ which is a wrong message for m_1.

Nearest Private Query

- Assuming two parties, a user (Bob) and a data owner (Alice).
- Bob has an input secrete parameter x. Lets assume $x = 8$.
- Alice has a private data set, $A = \{1, 2, 3, 6, 7, 10, 11, 14\}$.
- Bob wants to know which element (x_i) is the closest to x in Alice data set A, without revealing his secrete x.
- Alice cannot know anything about the secrete information x, and Bob cannot know secrete information about the private data set A except the near parameter, x_i.
- Alice generates a new set with $N = 2^n$ elements, $D(j)$ for $j = 0, 1, ...N - 1$ in which $D(j) = x_l$ being $x(l)$ the closest element to j in A. n is the number of bits that Alice needs to represent each element of her data set.

Nearest Private Query

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

- Bob and Alice have a set of keys K_i^* and K_i, respectively, with 64 elements where 60 are bits resulted from wrong basis measurement and 4 resulted from correct basis measurement. This allows Alice to know that Bob is being honest.
- Bob sends to Alice the set S with wrong bits position except in position $i = 8$.
- Alice gets the closest number to $x = 8$ which is 7 and she remains know nothing about the other elements.

QOKD with discrete variables

- Alice randomly generates the sets $S_{A1'}$ (for basis) and $S_{A2'}$ (for keys) in order to encode photons.
- Alice sends to Bob throughout a quantum channel l photons encoded using the previous values,

$$S_{AB} = \{\uparrow, \uparrow, \nearrow, \searrow, \searrow, \rightarrow, \rightarrow, \searrow, \nearrow, \uparrow, \rightarrow, \searrow, \nearrow, \searrow, \uparrow, \nearrow\}$$

- Bob also randomly generates $l = 16$ bits, which are going to define his measurement basis, $S_{B1'}$,

$$S_{B1'} = \{+, \times, \times, +, +, \times, +, \times, \times, +, \times, \times +, +, +, \times\}.$$

QOKD with discrete variables

- After measure the photons using the basis generated in $S_{B1'}$, he got $S_{B2'}$:

S_{AB}	$\uparrow$	$\uparrow$	$\nearrow$	$\searrow$	$\searrow$	$\rightarrow$	$\rightarrow$	$\searrow$	$\nearrow$	$\uparrow$	$\rightarrow$	$\searrow$	$\nearrow$	$\searrow$	$\uparrow$	$\nearrow$
$S_{B1'}$	$+$	$\times$	$\times$	$+$	$+$	$\times$	$+$	$\times$	$\times$	$+$	$\times$	$\times$	$+$	$+$	$+$	$\times$
$S_{B2'}$	1	$-$	$\underline{0}$	0	$-$	1	$\underline{1}$	$-$	1	$-$	1	0	1	1	$\underline{0}$	1

where "$-$" corresponds to no clicks in Bob's detector, due to attenuation and the underlined values to measurements with a correct basis but an error has occurred due to imperfections in the quantum communication system.

QOKD with discrete variables

- Bob sends to Alice,

$$S_{BH1} = \{S_1, -1, S_2, S_3, -1, S_4, S_5, -1, S_6, -1, S_7, S_8, S_9, S_{10}, S_{11}, S_{12}\},$$

where "-1" correspond to no clicks at the detector and the other values are Hash values calculated using SHA256.

- After Alice has received S_{BH1}, she sends throughout a classical channel the basis which she has used to codify the photons updated with the information about the no received photons.

- This way, due to attenuation them sets are reduced,

$$S_{A1} = \{0,1,1,0,0,1,0,1,1,1,0,1\},\ S_{A2} = \{1,1,0,0,0,1,0,0,1,0,1,1\},$$

$$S_{B1} = \{0,1,0,1,0,1,1,1,0,0,0,1\},\ S_{B2} = \{1,\underline{0},0,1,\underline{1},1,1,0,1,1,\underline{0},1\}$$

QOKD with discrete variables

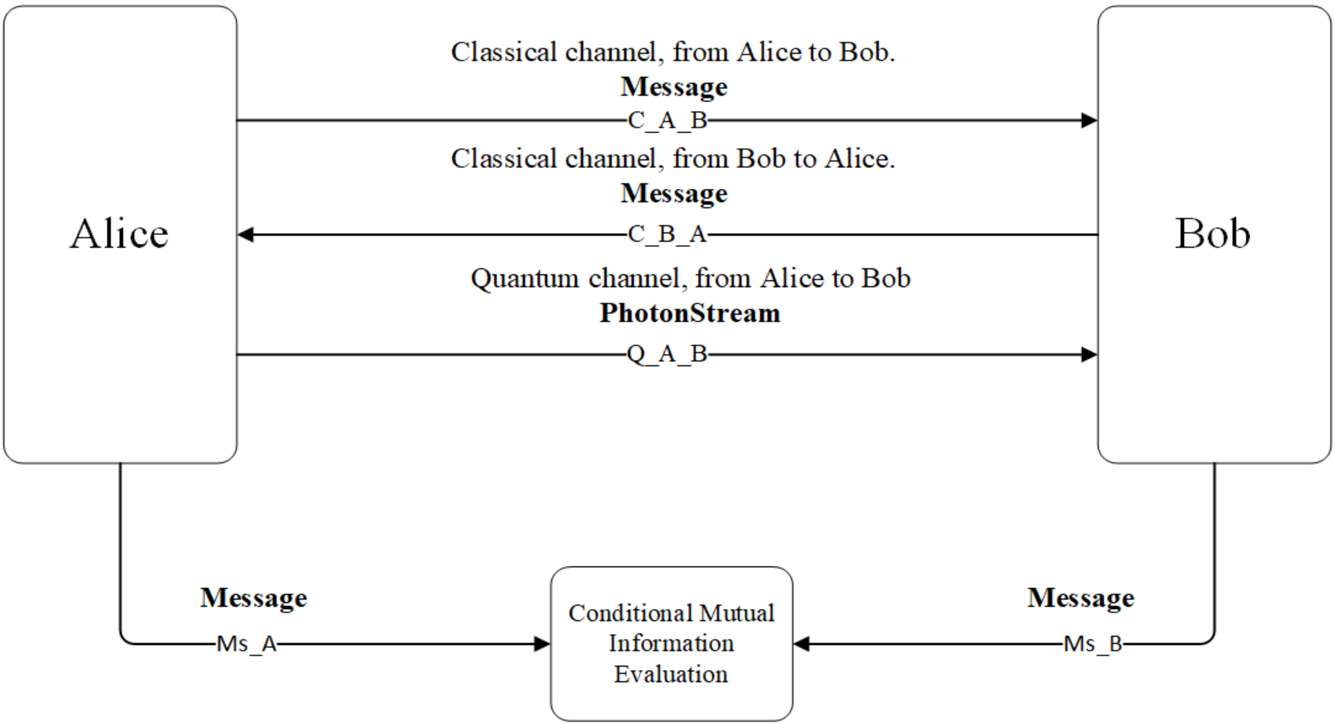
- Then, they apply a modified version of Cascade Algorithm in order to correct errors due transmission in the right set of measurements. Furthermore, they test the honesty of each other using the estimated QBER from Alice and the Hash Function committed by Bob.
- In order to know which photons were measured correctly, Bob does the operation $S_{B3} = S_{B1} \oplus S_{A1}$.
- Bob got $S_{B3} = \{1,1,0,0,1,1,0,1,0,0,1,1\}$.
- The values "1" correspond to the values he measured correctly and "0" to the values he just guessed.
- Bob is building two sets of keys, one with correct basis measurements values and other with the wrong basis measurement values that he just guessed.

QOKD with discrete variables

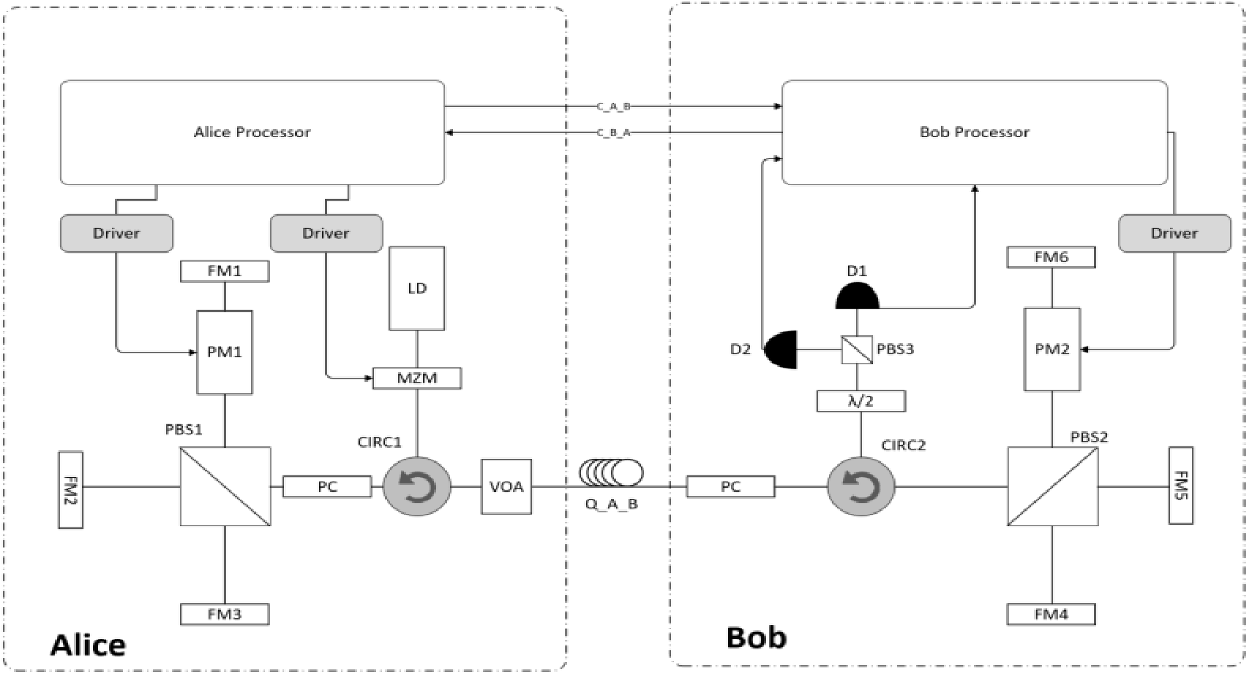
- By the end, Bob has four sets in order to have the capability of decode messages sent by Alice:

$$
\begin{aligned}
S_{B_{rp}} &= \{1,2,5,6,8\} \\
S_{B_{rb}} &= \{1,1,0,1,0\} \\
S_{B_{wp}} &= \{3,4,7,9\} \\
S_{B_{wb}} &= \{0,1,1,0\}
\end{aligned}
$$

Simulation Setup



Experimental Setup



E-mail: marianaferreiraramos@ua.pt