Universidade de Aveiro
2017-2018

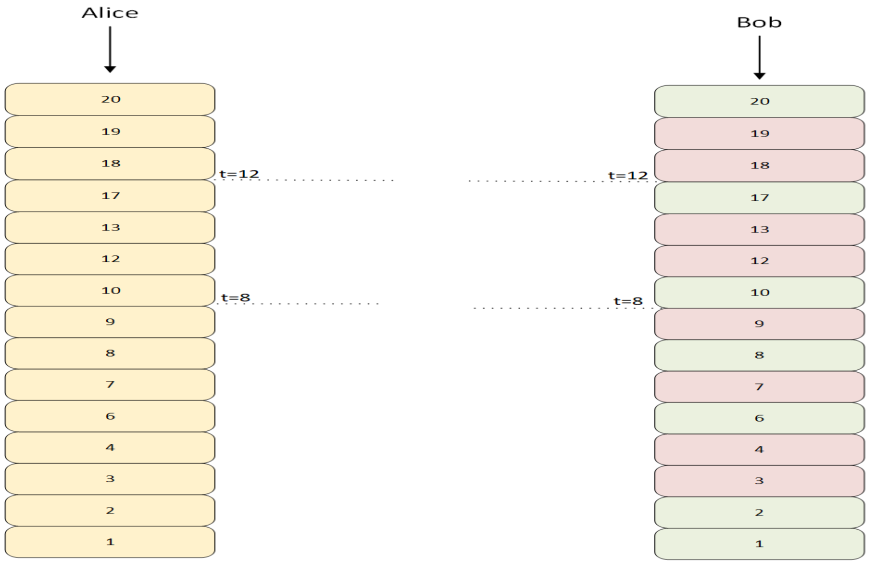
Quantum Oblivious Key Distribution with Discrete Variables

Mariana F. Ramos, Nuno A. Silva, Armando N. Pinto

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

Quantum Oblivious Key Distribution System (QOKD)

The QOKD system enables two parties (Alice and Bob) to share a set of keys. Only



Bob knows all information about the keys, which correspond to right or random bits. Alice only knows that half are right and half are random bits.

Quantum Oblivious Key Distribution System (QOKD)

From a QOKD system owe can obtain:

- Symmetric Secrete Keys.
- Oblivious Keys.
- Slightly Oblivious Keys.

Applications of a QOKD system

A QOKD system has applicability in two fields:

- Cryptography.
- Secure multi-party computation (1-out-of-2 Oblivious Transfer, Nearest Private Query).

Quantum Oblivious Key Distribution

Protocol detailed

QOKD - Protocol Detailed

Alice and Bob build them sets of keys continuously.

Step 1 Alice and Bob agree with a block length l. Lets assume $l = 16$. Lets assume Alice generates two sequences with l bits:

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

$$S_{A2'} = \{1,1,1,0,0,0,0,0,1,1,0,0,1,0,1,1\}.$$

where $S_{A1'}$ and $S_{A2'}$ are the sequence of basis and keys with which Alice will encode the photons, respectively.

QOKD - Protocol Detailed

Step 2 Alice sends to Bob throughout a quantum channel l encoded photons.

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

Step 3 Bob also randomly generates l bits to define his measurement basis. Lets assume:

$$\begin{aligned} S_{B1'} &= \{0\,,1\,,1\,,0\,,0\,,1\,,0\,,1\,,1\,,0\,,1\,,1\,,0\,,0\,,0\,,1\,\} \\ &= \{+, \times, \times, +, +, \times, +, \times, \times, +, \times, \times +, +, +, \times\}. \end{aligned}$$

Bob measures l photons and gets a new set,

$$S_{B2'} = \{1, -, \underline{0}, 0, -, 1, \underline{1}, -, 1, -, 1, 0, 1, 1, \underline{0}, 1\}.$$

where "$-$" corresponds to no clicks in Bob's detector, due to attenuation.

QOKD - Protocol Detailed

Step 4 Bob sends a "-1" or a hash value to Alice for each measurement that he performed. "-1" corresponds to the measurements when Bob had no clicks.

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

Step 5 After Alice has received S_{BH1}, she sends the basis set which she has used to encode the photons, updated with the information about the no received photons,

$$S_{A1'} = \{0, -1, 1, 1, -1, 0, 0, -1, 1, -1, 0, 1, 1, 1, 0, 1\}$$

.

QOKD - Protocol Detailed

Due to attenuation, the previous sets are reduced to the length 12 and they shall be replaced by the following:

$$
\begin{aligned}
S_{A1} &= \{0,1,1,0,0,1,0,1,1,1,0,1\},\\
S_{A2} &= \{1,1,0,0,0,1,0,0,1,0,1,1\},\\
S_{B1} &= \{0,1,0,1,0,1,1,1,0,0,0,1\},\\
S_{B2} &= \{1,\underline{0},0,1,\underline{1},1,1,0,1,1,\underline{0},1\}
\end{aligned}
$$

Note that S_{B2} still has errors.

QOKD - Protocol Detailed

Step 6 Bob does the operation $S_{B3} = S_{B1} \oplus S_{A1}$ to verify which photons he measured correctly,

$$S_{B3} = \{1,1,0,0,1,1,0,1,0,0,1,1\}.$$

Bob has been building two pair of sets, one for the right basis,

$$S_{B_{rp}} = \{1,2,5,6,8,11,12\},$$
$$S_{B_{rb}} = \{1,0,1,1,0,0,1\},$$

and other pair for photons he measured with the wrong basis and then he just guessed the values,

$$S_{B_{wp}} = \{3,4,7,9,10\},$$
$$S_{B_{wb}} = \{0,1,1,1,1\}.$$

QOKD - Protocol Detailed

In order to test Bob's honesty, Alice estimates the *QBER* of the channel. She must open a minimum number of right positions in order to guarantee a minimum *QBER*.

Alice chooses some positions to open and tells Bob which positions she wants to open.

Lets assume Alice has verified these pairs using the hash function committed by Bob and concluded that he is being honest. She sends to Bob the *QBER* estimated.

Bob has the previous sets replaced by the following,

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

QOKD - Protocol Detailed

Since some bits of $S_{B_{rb}}$ were wrongly measured, Bob must apply an error correction algorithm in order to correct the errors due transmission. As there are two sets with wrong and right bits, Bob has to apply a modified version of Cascade Algorithm. He applies the real cascade to $S_{B_{rb}}$ and a fake cascade version to $S_{B_{wb}}$. After applying the modified version of Cascade Bob gets,

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

Bob has to test Alice's honesty during the cascade algorithm by testing the validity of $QBER$ sent by her.

QOKD - Protocol Detailed

When Alice sends to Bob a photons set, they are building a set of pairs (array positions and bit values which correspond to measured photons at Bob's side and to the key bit with the photon was encoded at Alice's side).

The main goal is to guarantee that Bob has the same number of right and random pairs. In addition, they must know information about t.

Alice knows that at some tabs there are the same number of right and random bits.

1-out-of-2 Oblivious Transfer

Symmetric Oblivious Keys

1-out-of-2 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 $s = 4$ from them sets of keys:

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

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.

1-out-of-2 Oblivious Transfer

- Lets assume Bob wants to know m_0. He sends to Alice the set $S = \{I_r, Iw\}$.
- 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

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

1-out-of-2 Oblivious Transfer

- Bob uses values from $S_{B1'}$ at positions given by S and does the decrypted operation.

m	1	1	0	1	0	0	0	0
	1	1	1	0	0	1	1	0
$\oplus$	0	0	1	1	0	1	1	0

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

Asymmetric Oblivious Keys

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.

Nearest Private Query

- Alice generates a new set with $N = 2^n$ elements, $D(j)$ for $j = 0, 1, \ldots N-1$ 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.

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

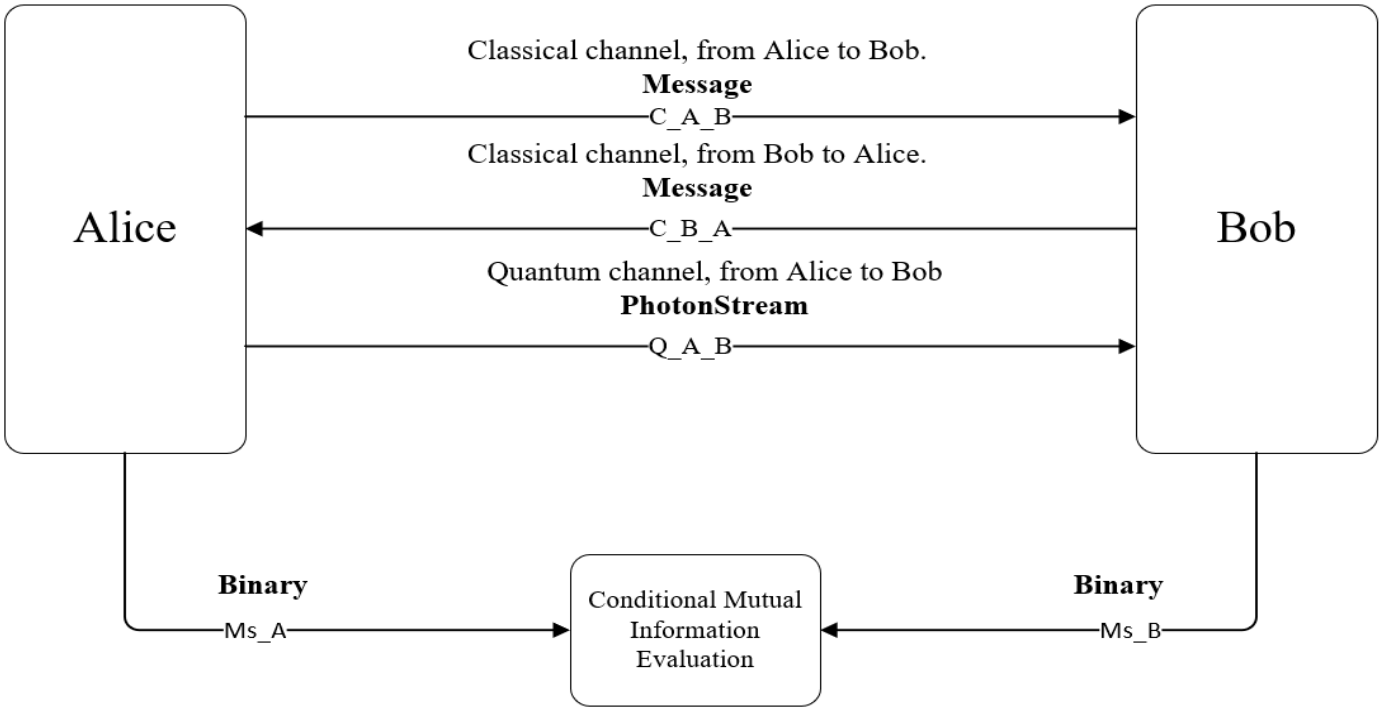
Nearest Private Query

- 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.

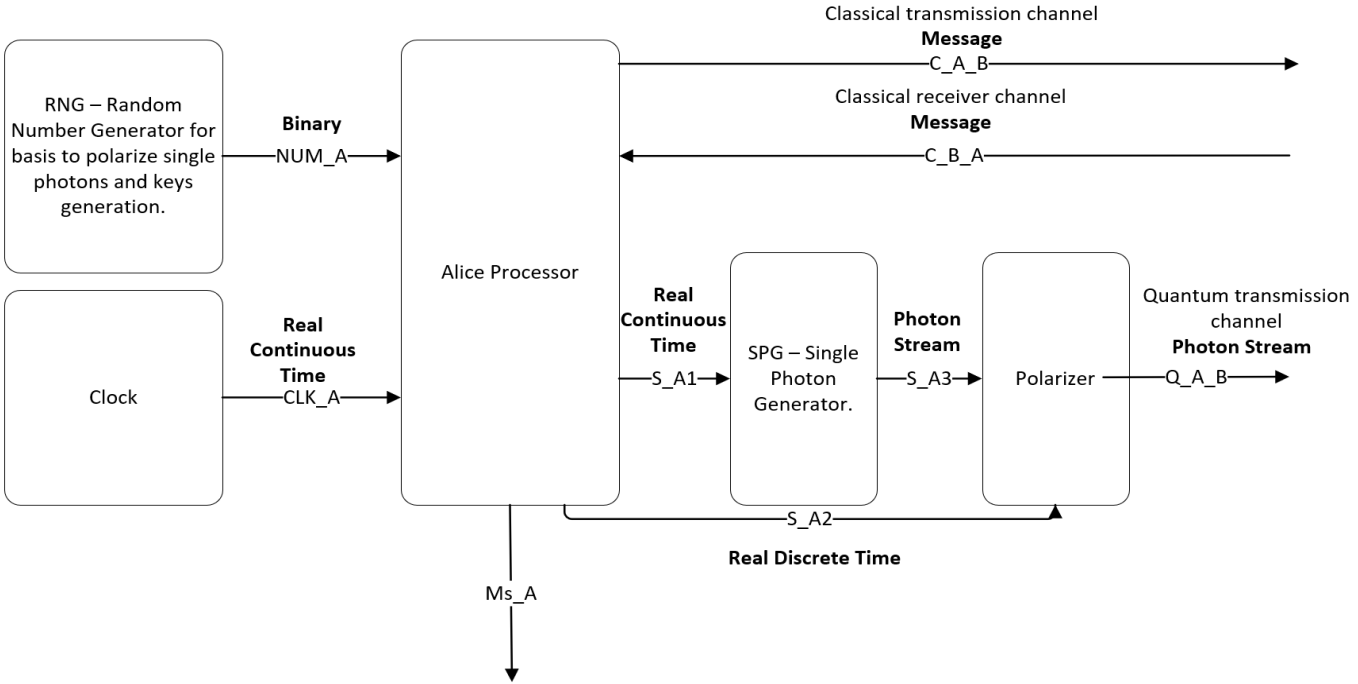
- Bob sends to Alice the set S with wrong bits positions except at $j = 8$.

- Alice gets the closest number to $x = 8$ which is 7 and she remains know nothing about the other elements.

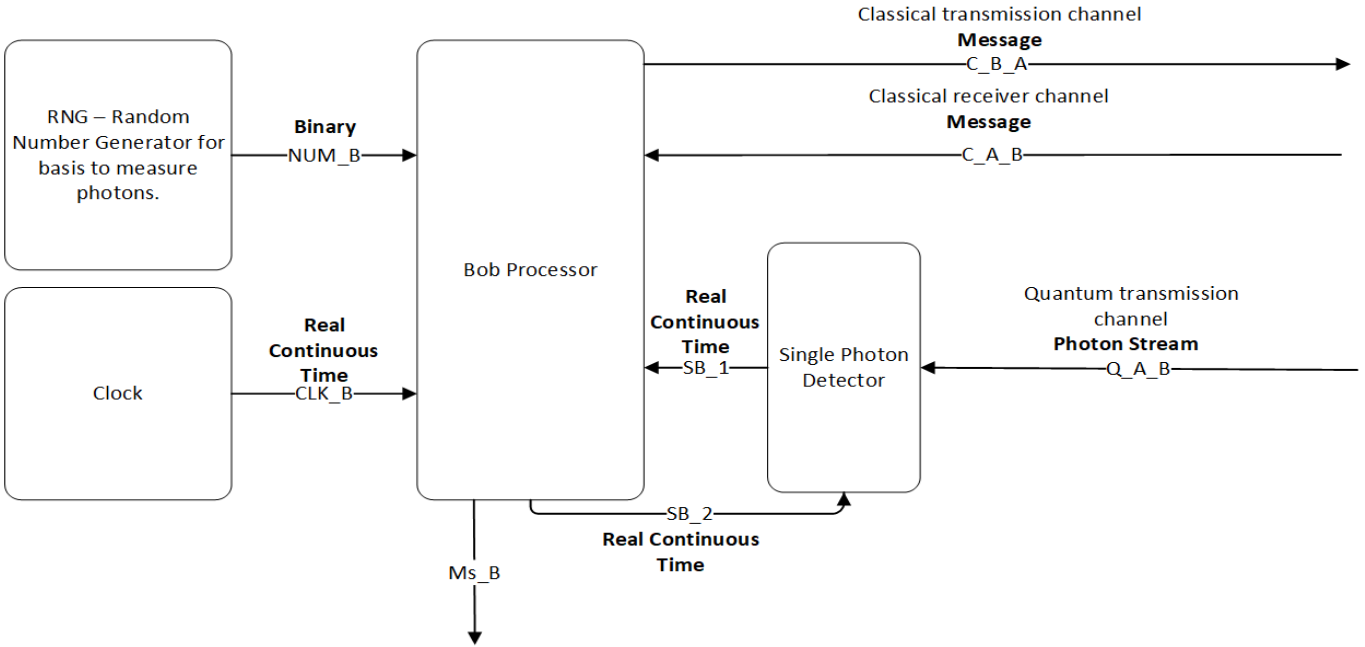
Simulation Setup



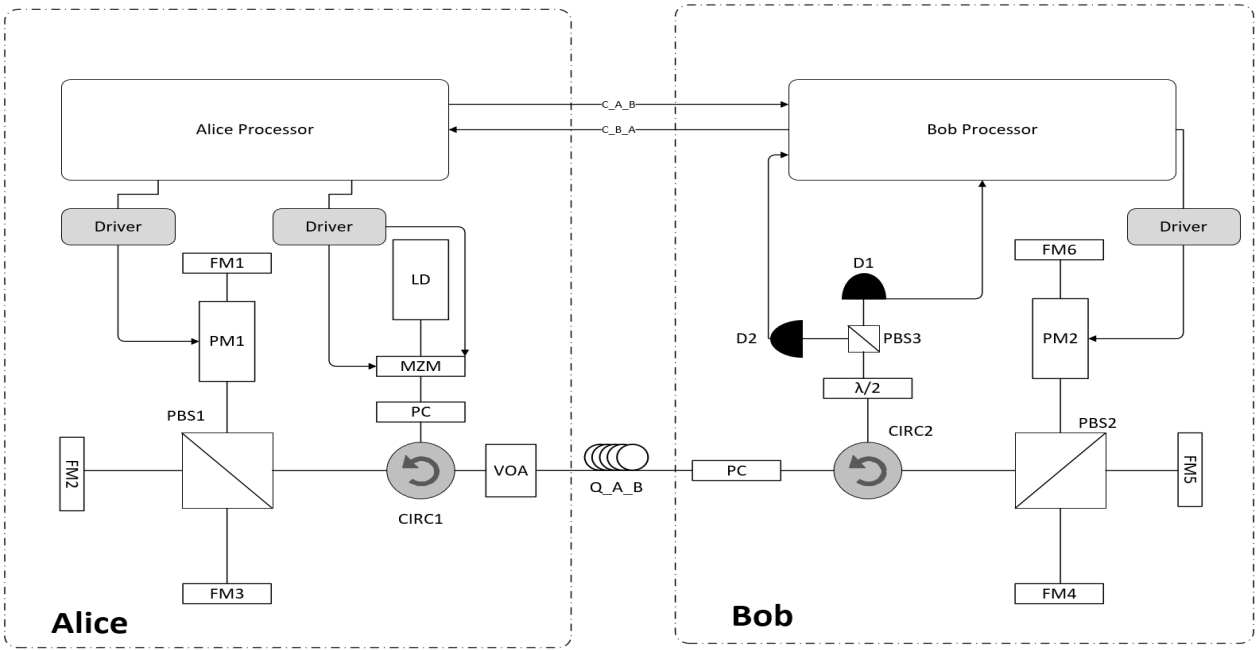
Simulation Setup - Alice



Simulation Setup - Bob



Experimental Setup



E-mail: marianaferreiraramos@ua.pt