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

1-out-of-2 OT Protocol: starting conditions

- Alice has two messages m_1 and m_2 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 $m_{\bar{b}}$.
- In order to implement OT between two parties (Alice and Bob) they must be able to exchange continuously oblivious keys, i.e a QOKD system must exist between them.
- Two basis are required: $'+'$ rectilinear basis and $'\times'$ diagonal basis. Lets assume,

	Basis "+"
0	$\rightarrow (0°)$
1	$\uparrow (90°)$

	Basis "$\times$"
0	$\searrow (-45°)$
1	$\nearrow (45°)$

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 keys.

Step 1 Set for both Alice and Bob the block length l. Lets assume $l = 16$. Lets assume Alice generates two sequences with l bits:

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

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

Quantum Oblivious Key Distribution System (QOKD)

Step 2 Alice sends to Bob throughout a quantum channel l photons encoded using the basis defined in $S_{A1'}$ and according to the key bits defined in $S_{A2'}$.

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

Step 3 Bob also randomly generates $l = 16$ bits, which are going 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 will get l results, where "$-$" corresponds to no clicks in Bob's detector, due to attenuation,

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

Quantum Oblivious Key Distribution System (QOKD)

Step 4 Bob is going to send a "-1" or a hash value (calculated by using SHA256 algorithm) to Alice for each measurement that he performed, thereby being "-1" the measurements which correspond to no clicks. Bob will send to Alice the following set:

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

Step 5 After Alice has received S_{BH1}, she sends throughout a classical channel the basis which she has used to codify the photons updated with the information about the no received photons,

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

Quantum Oblivious Key Distribution System (QOKD)

Step 5 - cont Due to attenuation, the previous sets are reduced to the length 12 and they shall be replaced by the following:

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

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

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

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

Note that S_{B2} still has errors.

Step 6 In order to know which photons were measured correctly, Bob does the operation $S_{B3} = S_{B1} \oplus S_{A1}$. He gets,

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

Quantum Oblivious Key Distribution System (QOKD)

Step 6 - cont Bob has been building two pair of sets, one for the right basis,

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

where $S_{B_{rp}}$ is the set of positions and SB_{rb} is the set of bit values he measured for each position. The other pair is for photons he measured with the wrong basis and then he just guessed the values,

$$S_{B_{wp}} = \{3,4,7,9,10\},$$

$$S_{B_{wb}} = \{0,1,1,1,1\},$$

where $S_{B_{wp}}$ is the set of positions and $S_{B_{wb}}$ is the set of bit values he measured for each position.

Quantum Oblivious Key Distribution System (QOKD)

Step 6 (cont) At this point, in order to test Bob's honesty and to estimate the *QBER* of the channel, Alice is going to ask Bob to open some pairs of the Bob's sets. She must open a minimum number of right position 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 and then she sends to Bob the *QBER* estimated.

Bob has the previous sets replaced by the following,

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

Quantum Oblivious Key Distribution System (QOKD)

Step 6 (cont) Since some bits of $S_{B_{rb}}$ were wrongly measured, Bob must apply an error correction algorithm in order to correct the error due transmission. In this case, as there are two sets with wrong and right bits, Bob has to apply a modified version of Cascade Algorithm. He will apply the real cascade to $S_{B_{rb}}$ and a fake cascade version to $S_{B_{wb}}$. Lets assume that after applying the modified version of Cascade Bob gets,

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

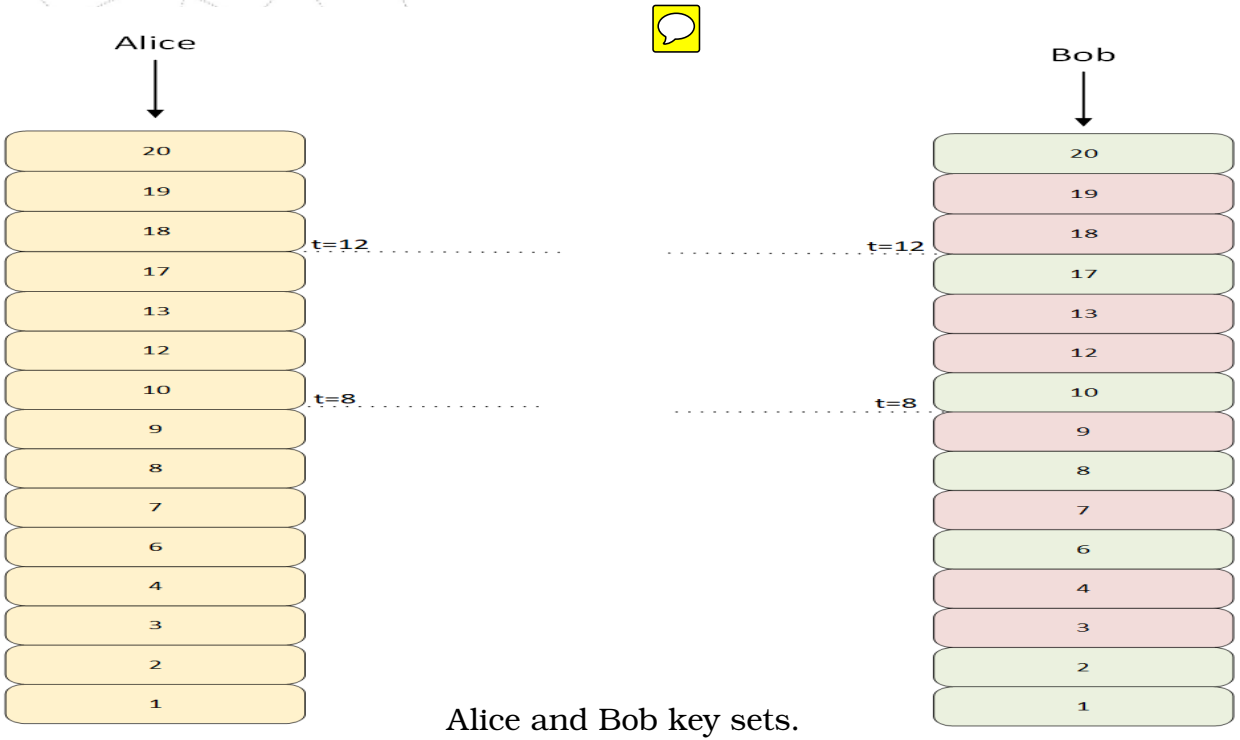
Quantum Oblivious Key Distribution System (QOKD)

Step 6 - cont Bob has to test Alice's honesty during the cascade algorithm by analysing the $QBER$ sent by Alice and if it is a realistic value.

Step 7 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 wrong pairs. In addition, they must know information about t.

Since Bob has sent to Alice the information about the smallest set, in this example, Alice know that there are four pairs of wrong positions and five pairs of right positions. Alice must destroy one of the right pairs by asking Bob to open it. Therefore, at $t = 8$ both know that there are the same number of right and wrong pairs thereby being the main goal guaranteed.

Quantum Oblivious Key Distribution System (QOKD)



Alice and Bob key sets.

OT Protocol with QOKD system

Alice sends two messages to Bob and he wants to know one of them. Alice does not know which message Bob wants and Bob only know the message he wants, i.e he does not know anything about the other message. Lets assume Alice send the following two messages with size $s = 4$, $m_0 = \{0011\}$ and $m_1 = \{0001\}$. As $t = 8$ Alice does not need to eliminate any bits.

Step 1 Bob defines two sub-sets with size $s = 4$:

$$I_0 = \{3,4,7,9\},$$

and

$$I_1 = \{1,2,6,8\},$$

where I_0 is the sequence of positions in which Bob was wrong about basis measurement and I_1 is the sequence of positions in which Bob was right about basis measurement.

OT Protocol with QOKD system

Step 2 Bob sends to Alice the set S_b. Lets assume he wants to know m_0, therefore he sends $S_0 = \{I_1, I_0\}$. Alice is sure about Bob's honesty, since she knows he only has 4 right basis to measure the photons. In addition, Alice cannot know which message Bob chose because she did not know the order that he sent the sets.

Step 3 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:

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

OT Protocol with QOKD system

Step 3 -cont Alice sends to Bob through a classical channel

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

Step 4 Bob uses $S_{B1\prime}$ values of positions given by I_1 and I_0 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 1 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.

E-mail: marianaferreiraramos@ua.pt