Universidade de Aveiro
2017-2018

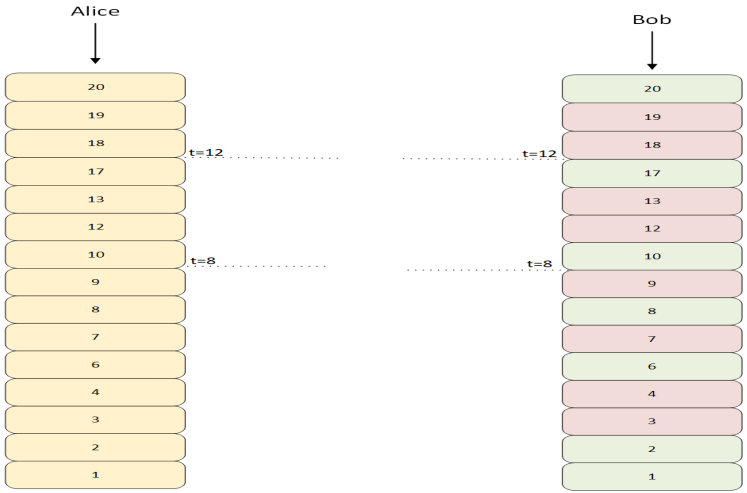
Quantum Oblivious Key Distribution with Discrete Variables

Mariana Ferreira Ramos
(marianaferreiraramos@ua.pt)

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

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.



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	$\nearrow (45°)$

1-out-of-2 OT Protocol with QOKD system

Lets assume Alice sends the following two messages with size $s = 4$, $m_0 = \{0011\}$ and $m_1 = \{0001\}$. At $t = 8$ 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.

1-out-of-2 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:

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

1-out-of-2 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}, 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.

Quantum Oblivious Key Distribution System (QOKD)

- Alice randomly generates the following 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, $S_{B1'}$,

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

Quantum Oblivious Key Distribution System (QOKD)

- 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.

Quantum Oblivious Key Distribution System (QOKD)

- 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,

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

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

Quantum Oblivious Key Distribution System (QOKD)

- 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.

Quantum Oblivious Key Distribution System (QOKD)

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

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

E-mail: marianaferreiraramos@ua.pt