Universidade de Aveiro
2016-2017

Oblivious Transfer Protocol with discrete variables (Polarization)

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 $m_{\bar{b}}$.
- First of all, Alice and Bob must know two parameters: message length s and the expansion factor k.
- Two basis are required: $'+'$ rectilinear basis and $'\times'$ diagonal basis.
- For rectilinear basis we defined as a binary 0 the polarization of 0° and a binary 1 the polarization of 90°.
- For diagonal basis we defined as a binary 0 the polarization of -45° and a binary 1 the polarization of 45°.

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

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

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

- Lets look an example: Alice has two messages to send to Bob: $m_0 = \{0011\}$ and $m_1 = \{0001\}$.
- Lets assume that in this example Alice and Bob knows two start parameters: the message's size $s = 4$ and a expansion factor $k = 2$.

1-out-of-2 OT Protocol: Description

Step 1 Alice randomly generates two bit sequences, with ks length:

S_{A1}	0	1	1	0	0	1	0	1	**Basis**
	+	×	×	+	+	×	+	×	

S_{A2}	1	1	0	0	0	1	0	0	**Keys**
	↑	↗	↘	→	→	↗	→	↘	

Step 2 Alice sends to Bob throughout a quantum channel ks photons encrypted using the basis defined in S_{A1} and according to the keys defined in S_{A2}.

$$S_{AB} = \{\uparrow, \nearrow, \searrow, \rightarrow, \rightarrow, \nearrow, \rightarrow, \searrow\}$$
$$S_{AB} = \{90°, 45°, -45°, 0°, 0°, 45°, 0°, -45°\}$$

1-out-of-2 OT Protocol: Description

Step 3 Bob also randomly generates ks bits. Lets assume:

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

When Bob receives photons from Alice, he measures them using the basis defined in S_{B1}:

$$\{+,\times,+,\times,+,\times,\times,\times\}$$

Bob will get ks results:

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

1-out-of-2 OT Protocol: Description

Step 4 Bob will send a *Hash Function* result HASH1 to Alice. This value will do Bob's commitment with the measurements done. In this case, this *Hash Function* is calculated from *SHA-256* algorithm for each pair (Basis from S_{B1} and measured value from $S_{B1'}$).

Step 5 When Alice receives HASH1, she sends throughout a classical channel the basis she used to encode the photons. In this case, we have assumed:

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

1-out-of-2 OT Protocol: Description

Step 6 In order to know if he measured the photons correctly, Bob does the operation $S_{B2} = S_{B1} \oplus S_{A1}$.

S_{B1}	0	1	0	1	0	1	1	1
S_{A1}	0	1	1	0	0	1	0	1
$\oplus$	1	1	0	0	1	1	0	1

The values $'1'$ correspond to the values he measured correctly and $'0'$ to the values he just guessed. Thus, $S_{B2} = \{1,1,0,0,1,1,0,1\}$. Bob needs to send to Alice, through a classical channel, $n = min(\#0, \#1) = 3$, where $\#0$ represents the number of zeros in S_{B2} and $\#1$ the number of ones in S_{B2}. In order to prove his honesty and to prove that he is not cheating Alice, Bob must send to Alice a value (resulted from an Hash Function), such that she can know n from this function.

1-out-of-2 OT Protocol: Description

Step 6 (cont) At this time, Alice must be able to know if Bob is being honest or not. Therefore, she will open Bob's commitment from *step 4* and she verify if the number n sent by Bob is according with the commitment values sent by him.

Step 7 If $n < s$, Alice and Bob will repeat the steps from 1 to 7. In this case, $n = 3$ which is smaller than $s = 4$. Therefore, Alice and Bob repeat the steps from 1 to 7 in order to enlarge Bob's sets S_{B1} and S_{B2} as well as Alice's sets S_{A1} and S_{A2}.

Step 8 Lets assume :

$$S_{B1} = \{1,1,0,0,0,1,0,0,1,0,0,0,0,0,1,1\},$$
$$S_{A1} = \{0,1,1,0,0,1,0,1,1,1,0,0,1,1,1,0\},$$
$$S_{A2} = \{1,1,0,0,0,1,0,0,1,0,1,0,0,0,1,1\}.$$

1-out-of-2 OT Protocol: Description

Step 8 (cont) Finally, for $S_{B2} = S_{B1} \oplus S_{A1}$:

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

Note that the sets were enlarge in the second iteration.

Step 9 At this time, Bob sends again to Alice, through a classical channel, $n = min(\#0, \#1) = 7$.

Step 10 Alice checks if $n > s$ and acknowledge to Bob that she already knows that $n > s$. In this case, $n = 7$ and $s = 4$ being $n > s$ a valid condition.

1-out-of-2 OT Protocol: Description

Step 11 Bob defines two new sub-sets, I_0 and I_1.In this example, Bob defines two sub-sets with size $s = 4$:

$$I_0 = \{3,4,7,11\}, I_1 = \{2,5,6,13\}.$$

Bob sends to Alice the set S_b. If Bob wants to know m_0 he must send to Alice throughout a classical channel the set $S_0 = \{I_1, I_0\}$, otherwise if he wants to know m_1 he must send to Alice throughout a classical channel the set $S_1 = \{I_0, I_1\}$.

Step 12 With both the received set S_b and the hash function value HASH1, Alice must be able to prove that Bob has been being honest.

1-out-of-2 OT Protocol: Description

Step 13 Lets assume Bob sent $S_0 = \{I_1, I_0\}$. Alice defines two encryption keys K_0 and K_1 using the values in positions defined by Bob in the set sent by him. In this example, lets assume:

$$K_0 = \{1,0,1,0\} \text{ and } K_1 = \{0,0,0,1\}.$$

Alice does the operation $m = \{m_0 \oplus K_0, m_1 \oplus K_1\}$.

m_0	0	0	1	1		m_1	0	0	0	1
K_0	1	0	1	0		K_1	0	0	0	1
$\oplus$	1	0	0	1		$\oplus$	0	0	0	0

Adding the two results, Alice will send to Bob the encoded message $m = \{1,0,0,1,0,0,0,0\}$.

1-out-of-2 OT Protocol: Description

Step 14 When Bob receives the message m, in the same way as Alice, Bob uses $S_{B1'}$ values of positions given by I_1 and I_0 and does the decrypted operation:

m	1	0	0	1	0	0	0	0
	1	0	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.

1-out-of-2 OT Protocol: Open Issues

Steps 4 and 12 are not fully defined.

1. In step 4 Bob may says to Alice that he has already measured the photon and it could be a lie. In order to prevent this an Hash Function must be used.
2. In step 12 Bob may uses some values in a dishonest way, i.e Bob can pick values from I_1 which he knows they are correct and send them in I_0 in order to know correct information about message $m_{\bar{b}}$.

This problems can hopefully be solved using *Bit Commitment* through *Hash Functions*.

E-mail: marianaferreiraramos@ua.pt