1 Quantum Multi-Party Computation

1.1 Our Approach

1.1.1 1 out of 2 Oblivious Transfer

This section will provide the description of a 1-2 Oblivious Transfer (OT) based on the appliance of a Quantum Oblivious Key Distribution Protocol (QOKD). The 1-2 OT consists in a two party, Alice and Bob, communication protocol. Supposing that Alice has two messages $\{m_1, m_0\}$ length s, Bob wants to know one of those in such a way that:

- Alice doesn't know Bob's choice, i.e. the protocol is oblivious;
- Bob doesn't get any information on the message he didn't choose, i.e. the protocol is concealing.

Considering the notation of a canonical quantum oblivious transfer protocol, let $U = \{+, \times\}^n \times \{0,1\}^n$, where $+, \times$ stand for the rectilinear and diagonal bases, with a correspondence previously agreed by both Bob and Alice. Physically this corresponds The general algorithm of the protocol can be described as:

- Step 1:
  Alice picks a random uniformly chosen $\big(a, g\big) \in U$, and sends Bob photons i, $1 \leq i \leq n$ with polarizations given by the bases $a\big[i\big]$ and states $g\big[i\big]$.
- Step 2:
  Bob picks a random uniformly chosen $b \in \{+, \times\}^n$, measures photons i in basis $b\,[i]$ and records the results, if a photon is detected, as $h\,[i] \in \{0,1\}$. Bob then makes a bit commitment of all n pairs $(b\,[i]\,, h\,[i])$ to Alice.
- Step 3:
  Alice picks a random uniformly picks a random uniformly chosen subset $R \subset \{1, 2, ..., n\}$ and tests the commitment made by Bob at positions in R. If more δn (acceptance threshold) positions $i \in R$ reveal $a\,[i] = b\,[i]$ and $g\,[i] \neq h\,[i]$ then Alice stops protocol; otherwise, the test result is accepted.
- Step 4:
  Alice announces the base a. Let T_0 be the set of $1 \leq i \leq n$ such that $a\,[i] = b\,[i]$ and let T_1 be the set of all $1 \leq i \leq n$ such that $a\,[i] \neq b\,[i]$. Bob chooses $I_0, I_1 \subset T_0 - R, T_1 - R$ and sends $S_i = \{I_{1-i}, I_i\}$, wishing to know m_i, $i \in \{0,1\}$.
- Step 5:
  Alice defines two encryption keys K_0, K_1 in such a way that $K_i = g\big[I_i\big]$ for $i = 0 \vee i = 1$. Alice then cyphers both messages: $m_{\texttt{coded}} = \{m_0 \oplus K_0, m_1 \ \oplus K_1\}$ and sends the result m to Bob.
- Step 6:
  Bob will then decode m using the values of his initially chosen basis: $b\,[S_i]$ with $i \in \{0,1\}$, according to his preference. $m_{\texttt{decoded}} = m_{\texttt{coded}} \oplus b\,[S_i]$. The output of this process will be $m_{\texttt{decoded}}$ that will have the correct message in the first or last s^{th} positions if he chose m_0 or m_1, respectively.

It is intuitively clear that the above protocol performs correctly if both parties are honest [**?**]. The security of protocol depends, though on the honesty of both parties (and a potential eavesdropper) involved. The security of the protocol can be evaluated in terms of the amount of information received by any given participant. In order to formalize and proof the security of such a system for any case though one has to think of the proceedings of a hypothetically dishonest Bob and an eventual eavesdropper Eve.

- Step 1:
  Dishonest Bob has no advantage in being dishonest at this point.

- Step 2:
  Dishonest Eve transfers some information from this pulse into her quantum system and she uses that information to modify the residual state of the pulse which is sent to Bob.
  Dishonest Bob executes a coherent measurement on the pulse received in order to determine: whether or not he declares this pulse as detected and the bit that he commits to Alice.

- Step 4:
  Having learnt Alice's string of basis a dishonest Bob executes a first post-measurement of his choice and uses the outcome to compute the ordered pair S.

- Step 5:
  Using the information obtained in the previous step dishonest Bob makes a second post-test measurement and obtains the outcome $\mathcal{J}_{Bob}$. Eve measures her system and obtains the outcome $\mathcal{J}_{Eve}$ [**?**].

From [**?**] one can concluded that a dishonest Bob following these proceedings learns nothing about m, the set of both original messages concatenated, in its full extended, either he passes or fails Alice's original verification. This protocol also compensates the errors in the quantum channel. It is also stated that security against Bob and tolerance against errors implies the security of the protocol against Eve [**?**].