Quantum key distribution with entangled qubits

Bruno Fédrici

October 1, 2024

This project is based on the paper Quantum Cryptography with Entangled Photons from T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger published in 1999. It describes the establishment of highly secure keys through the manipulation of polarization entangled photon pairs.

1 The protocol

In class, we studied the BB84 protocol as an example quantum key distribution (QKD) protocol. It relies on the distribution and the manipulation of single qubits. However, as an alternative approach, one can also share secret keys using entangled qubit pairs rather than single qubits.

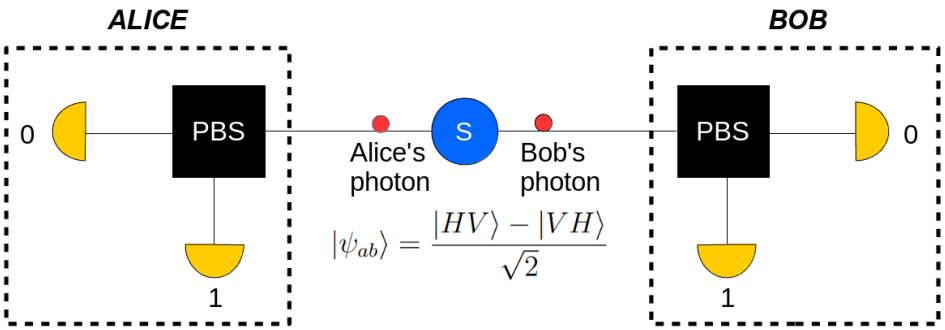
The basic idea behind QKD with entangled qubit pairs consists in exploiting the strong correlations of qubits prepared in an entangled state to establish a key, but also to monitor the security of the protocol.

1.1 Key establishement

For instance, in the aforementioned paper from Zeilinger et al., the authors described a setup in which a source of polarization entangled photon pairs is positioned halfway to Alice and Bob so as to distribute one photon from the pair to Alice, and the other one to Bob. Since this source emits pairs in state

$$|\psi_{ab}\rangle = \frac{|HV\rangle - |VH\rangle}{\sqrt{2}},$$

if Alice and Bob both measure their respective qubits in the $\{|H\rangle, |V\rangle\}$ basis, then Alice's measurement outcomes will be perfectly anti-correlated with Bob's measurement outcomes, i.e. they share a key.

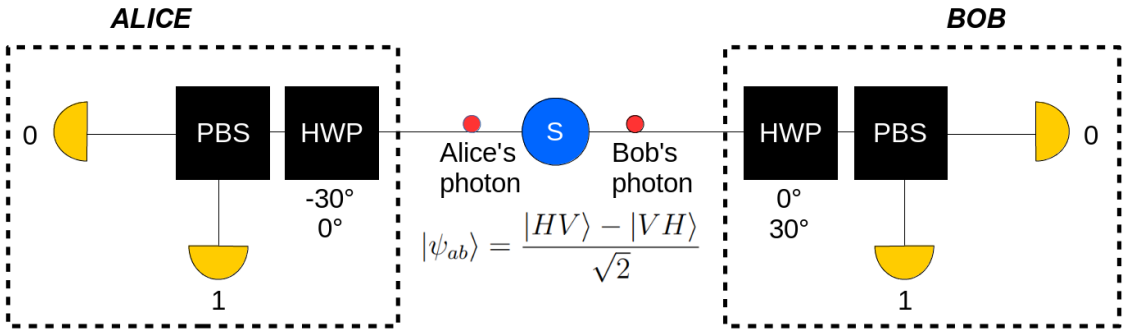


In an optical setup, such a measurement can be achieved throug using a Polarizing Beam Splitter (PBS) followed by a single-photon detector on both output of the PBS. If a photon enter the PBS in state $|H\rangle$ (respectively $|V\rangle$), then this photon has 100% chance to be transmitted (respectively reflected), in which case the first (respectively second) detector "click" and a 0 (respectively a 1) is registered.

1.2 Security of the protocol

Suppose Eve, an eavesdropper, is tapping in the quantum channel so as to gain information on the key. Every time Eve performs a measurement on a qubit pair, the state of the pair after Eve's measurement is no longer an entangled state but a product state. And so, to guess if a third party was listening or not, the only thing Alice and Bob have to do, is to find a way to discriminate in between a product state and an entangled state. Hopefully, this can be achieved through using extra measurement basis.

In an optical setup, changing the measurement basis can be achieved through adding and rotating a half-waveplate (HWP) in front of the PBS. If the orientation of the HWP is 0°, one can then discriminate in between $|H\rangle$ and $|V\rangle$ thanks to the PBS as we did before. Now, suppose you want to discriminate, in between the $|D\rangle = \frac{|H\rangle + |V\rangle}{\sqrt{2}}$ (diagonal) and $|A\rangle = \frac{|H\rangle - |V\rangle}{\sqrt{2}}$ (anti-diagonal) polarization states instead of $|H\rangle$ and $|V\rangle$. Then, the only thing to do is to rotate the HWP of 45° .



To ensure the security of the protocol, the authors of the paper propose that Alice (respectively Bob) randomly switches the orientation of her (his) HWP in between -30° and 0° (respectively 0° and 30°) from one photon pair to another. Measurements in parallel orientations (0°, 0°) are used to generate a key - as already explained, while measurements in non-parallel orientations (-30°, 0°), (0°, 30°), and (-30°, 30°) are used to compute the following quantity:

$$W = p(a = 0, b = 0| - 30°, 0°) + p(a = 0, b = 0|30°, 0°) - p(a = 0, b = 0| - 30°, 30°)$$

$p(a = 0, b = 0| - 30°, 0°)$ is the joint probability that Alice get a bit 0 (i.e. her photon is transmitted) when her HWP is oriented at -30° and Bob get a 0 (i.e. his photon is transmitted) when his HWP is oriented at 0°.

For the maximally entangled state $|\psi_{ab}\rangle$, the quantum theory predicts that $p(a = 0, b = 0| - 30°, 0°) = p(a = 0, b = 0|30°, 0°) = 1/8$ and $p(a = 0, b = 0| - 30°, 30°) = 3/8$, and so $W = -1/8$. However, for a product state, the quantum theory predicts that W is no longer negative, but positive.

Consequently, if W is negative, the shared key (i.e. the bits obtained with parallel orientations) is actually a secret key that can later be used for encryption. In the opposite case, if W is positive, the shared key can no longer be used as someone listened and a new batch of data must be generated.

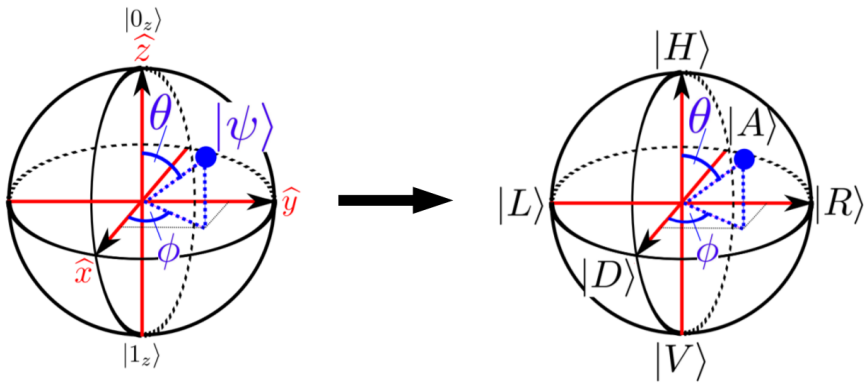
2 Implementation in Qiskit

2.1 Mapping in the Bloch sphere

This protocol canbe simulated using a quantum library like Qiskit. For that, one first needs to translate quantum optics vocabulary into hardware agnostic quantum computing vocabulary. First of all, one can map the polarization states onto the Bloch sphere with the mapping

$$Z\text{-basis} \begin{cases} |H\rangle \Longleftrightarrow |0\rangle \\ |V\rangle \Longleftrightarrow |1\rangle \end{cases} \quad X\text{-basis} \begin{cases} |D\rangle \Longleftrightarrow |+\rangle \\ |A\rangle \Longleftrightarrow |-\rangle \end{cases} \quad Y\text{-basis} \begin{cases} |R\rangle \Longleftrightarrow |+i\rangle \\ |L\rangle \Longleftrightarrow |-i\rangle \end{cases} \tag{1}$$

where $|R\rangle$ and $|L\rangle$ stand for right and left circular polarization states respectively. The mapping is illustrated in this figure:



The action of the HWP can then be simulated using a R_y gate prior to measurement. Accessing circular polarization states would have necessitate a quarter-waveplate (QWP) in addition to the HWP, an extra optical component equivalent to a R_z gate. However, there is no need of R_z gate here since the focus of the protocol is on linear polarization states - the states located in the xz-plan of the sphere.

2.2 Reproducing the protocol step-by-step

You are now ready to build a quantum program in Qiskit simulating the QKD protocol. So for that, please proceed the following way:

1. Instantiate a `QuantumCircuit` of two qubits and two classical bits, and set those qubits in the entangled state

$$|\psi_{ab}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

2. Instantiate four new `QuantumCircuit` objects of two qubits and two classical bits, and add necessary instructions in those circuits for those circuits to mimic photon pair measurements in orientations (0°, 0°), (-30°, 0°), (0°, 30°), and (-30°, 30°).

3. Generate two random bit-strings of size 1024 for Alice and Bob measurement settings respectively.

4. Repeat 1024 times the process of first composing the entangling circuit with one of the four measurement circuits and then running one time the composed circuit. Here, the measurement circuit must be selected at random - otherwise an eavesdropper can guess what Alice and Bob are doing, so for that use the random bit-strings previously generated. One can agree on the following mapping for the measurement settings:

   - $(0°, 0°) \rightarrow$ Alice:0, Bob:0
   - $(-30°, 0°) \rightarrow$ Alice:1, Bob:0
   - $(0°, 30°) \rightarrow$ Alice:0, Bob:1
   - $(-30°, 30°) \rightarrow$ Alice:1, Bob:1

5. Save in a list Alice (or Bob) measurement outcomes obtained in configuration $(0°, 0°)$, i.e. the key.

6. From the measurement outcomes obtained in other configurations, compute $p(a = 0, b = 0| - 30°, 0°)$, $p(a = 0, b = 0|30°, 0°)$ and $p(a = 0, b = 0| - 30°, 30°)$. Finally, compute W.

7. Display the key, the three aforementioned probabilities, and the value of W for this data batch.

8. Until the user decide to stop your program, repeat again and again the previous steps with, every time, a new batch of size 1024.

9. Every time a new batch is processed, add the value of W on a graph "W vs Batch ID".

10. To simulate an eavesdropper, add the possibility, for every new batch, to start with a product state (e.g. $|01\rangle$) instead of an entangled state.

11. Finally, raise an alert "Alert : someone is listening !" every time W reaches a positive value.