Quantum project: Report 1

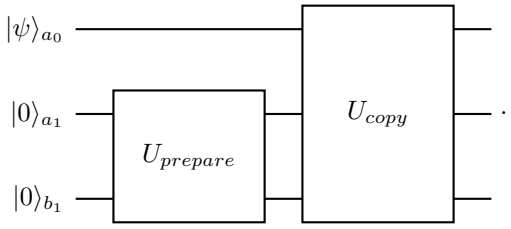
December 7, 2020

1 Introduction

Copying arbitrary quantum information is forbiden by the laws of quantum mechanics. Quantum communication protocols, e.g. QKD, rely on the fact that an eveasdroper will be noticed when intercepting and reading the information, which ensures that communication remains private. In this work we explore an imperfect quantum copy machine and its implementation on quantum computing platforms such as Quantum Inspire (QI). First, we will analyze the circuit that implements this copy machine and obtain a clear idea of what the output state is. Secondly, we implement this circuit for all single qubit states and show the results of the devices Starmon5 and the QXsimulator.

2 Universal quantum copy machine

The quantum circuit corresponding to the UQCM contains two stages, as can be seen in the following circuit,

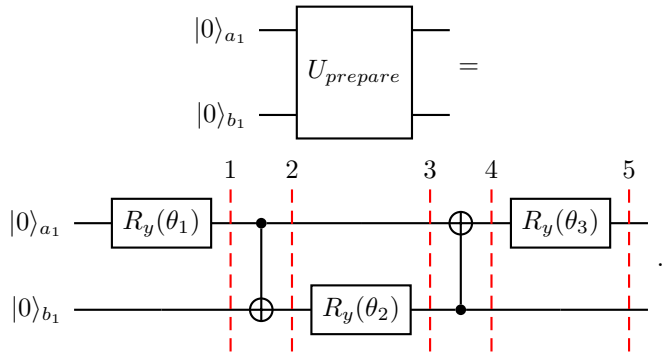


2.1 Preparation of the state

The first stage of the UQCM starts before interacting with the input qubit. The two bottom qubits are required to be in an arbitrary state,

$$|\phi\rangle_{a_1 b_1} = C_1|00\rangle + C_2|01\rangle + C_3|10\rangle + C_4|11\rangle. \tag{1}$$

For such purpose we will use the following circuit with an input state $|00\rangle_{a_1 b_1}$.



We analyse each stage of the preparation process. Simply denote $|00\rangle_{a_1 b_1}$ as $|00\rangle$, where the qubit from left to right side is always $a_1 b_1$.

The rotation gate here is defined by

$$R_y(\theta) = \cos(\theta/2)\hat{I} - i\sin(\theta/2)\hat{Y} = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

And the formula can be given by,

$$\begin{aligned}
|\phi_0\rangle &= |00\rangle \\
|\phi_1\rangle &= (\cos(\theta_1/2)|0\rangle + \sin(\theta_1/2)|1\rangle)|0\rangle \\
|\phi_2\rangle &= \cos(\theta_1/2)|00\rangle + \sin(\theta_1/2)|11\rangle \\
|\phi_3\rangle &= \cos(\theta_1/2)|0\rangle(\cos(\theta_2/2)|0\rangle + \sin(\theta_2/2)|1\rangle) + \sin(\theta_1/2)|1\rangle(-\sin(\theta_2/2)|0\rangle + \cos(\theta_2/2)|1\rangle) \\
&= \cos(\theta_1/2)\cos(\theta_2/2)\,|00\rangle + \cos(\theta_1/2)\sin(\theta_2/2)\,|01\rangle - \sin(\theta_1/2)\sin(\theta_2/2)\,|10\rangle + \sin(\theta_1/2)\cos(\theta_2/2)\,|11\rangle \\
|\phi_4\rangle &= \cos(\theta_1/2)\cos(\theta_2/2)|00\rangle + \cos(\theta_1/2)\sin(\theta_2/2)|11\rangle - \sin(\theta_1/2)\sin(\theta_2/2)|10\rangle + \sin(\theta_1/2)\cos(\theta_2/2)|01\rangle \\
|\phi_5\rangle &= (\cos(\theta_3/2)|0\rangle + \sin(\theta_3/2)|1\rangle)(\cos(\theta_1/2)\cos(\theta_2/2)|0\rangle + \sin(\theta_1/2)\cos(\theta_2/2)|1\rangle) \\
&\quad + (-\sin(\theta_3/2)|0\rangle + \cos(\theta_3/2)|1\rangle)(\cos(\theta_1/2)\sin(\theta_2/2)|1\rangle - \sin(\theta_1/2)\sin(\theta_2/2)|0\rangle)
\end{aligned}$$

Finally, we found that the coefficients of the final state depends on the rotation angles,

$$|\phi\rangle = C_1|00\rangle + C_2|01\rangle + C_3|10\rangle + C_4|11\rangle.$$

From which we can observe that,

$$C_1 = \sin(\theta_1/2)\sin(\theta_2/2)\sin(\theta_3/2) + \cos(\theta_1/2)\cos(\theta_2/2)\cos(\theta_3/2) \quad (2)$$
$$C_2 = \sin(\theta_1/2)\cos(\theta_2/2)\cos(\theta_3/2) - \cos(\theta_1/2)\sin(\theta_2/2)\sin(\theta_3/2) \quad (3)$$
$$C_3 = \cos(\theta_1/2)\cos(\theta_2/2)\sin(\theta_3/2) - \sin(\theta_1/2)\sin(\theta_2/2)\cos(\theta_3/2) \quad (4)$$
$$C_4 = \sin(\theta_1/2)\cos(\theta_2/2)\sin(\theta_3/2) + \cos(\theta_1/2)\sin(\theta_2/2)\cos(\theta_3/2) \quad (5)$$

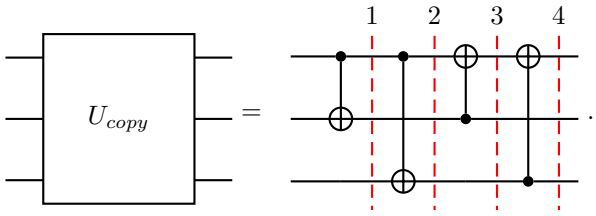
In order to obtain the desiered preparation state described in the following section, the following angles were used:

$$\cos(\theta_1) = \frac{1}{\sqrt{5}}, \quad \cos(\theta_2) = \frac{\sqrt{5}}{3}, \quad \cos(\theta_3) = \frac{2}{\sqrt{5}}$$

2.2 Copying proccess

Once we have prepared the state, we do the copy process, which can be described as controlled entanglement between the input and prepared qubits. The circuit corresponding to the copy process can be observed in the following circuit, where the prepared initial state and the input state that we consider are given respectively by,

$$|\phi\rangle_{a_1,b_1}^{(prep)} = \frac{1}{\sqrt{6}}(2|00\rangle + |01\rangle + |11\rangle), \qquad |\psi\rangle_{a_0}^{(in)} = \alpha|0\rangle + \beta|1\rangle. \tag{6}$$



We consider that the input state of the copy machine is $|\Psi_0\rangle = |\psi\rangle_{a_0}^{(in)}|\phi\rangle_{a_1,b_1}^{(prep)}$. Then, it will transform in each stage of the copy process as,

$$|\Psi_1\rangle = \frac{\alpha}{\sqrt{6}}|0\rangle(2|00\rangle + |01\rangle + |11\rangle) + \frac{\beta}{\sqrt{6}}|1\rangle(2|10\rangle + |11\rangle + |01\rangle) \tag{7}$$

$$|\Psi_2\rangle = \frac{\alpha}{\sqrt{6}}|0\rangle(2|00\rangle + |01\rangle + |11\rangle) + \frac{\beta}{\sqrt{6}}|1\rangle(2|11\rangle + |10\rangle + |00\rangle) \tag{8}$$

$$= \sqrt{\frac{2}{3}}(\alpha|000\rangle + \beta|111\rangle) + \frac{1}{\sqrt{6}}(\alpha|001\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|100\rangle) \tag{9}$$

$$|\Psi_3\rangle = \sqrt{\frac{2}{3}}(\alpha|000\rangle + \beta|011\rangle) + \frac{1}{\sqrt{6}}(\alpha|001\rangle + \alpha|111\rangle + \beta|010\rangle + \beta|100\rangle) \tag{10}$$

$$|\Psi_4\rangle = \sqrt{\frac{2}{3}}(\alpha|000\rangle + \beta|111\rangle) + \frac{1}{\sqrt{6}}(\alpha|101\rangle + \alpha|011\rangle + \beta|010\rangle + \beta|100\rangle) \tag{11}$$

$$= \left(\sqrt{\frac{2}{3}}\alpha|00\rangle + \beta\frac{1}{\sqrt{6}}(|10\rangle + |01\rangle)\right)|0\rangle + \left(\sqrt{\frac{2}{3}}\beta|11\rangle + \frac{1}{\sqrt{6}}\alpha(|10\rangle + |01\rangle)\right)|1\rangle \tag{12}$$

$$= |\chi_0\rangle|0\rangle + |\chi_1\rangle|1\rangle \equiv |\Psi\rangle\,, \tag{13}$$

where we have defined

$$|\chi_0\rangle = \sqrt{\frac{2}{3}}\alpha|00\rangle + \sqrt{\frac{1}{3}}\beta|\Phi_+\rangle = \sqrt{\frac{2}{3}}\alpha\,|00\rangle + \sqrt{\frac{1}{6}}\beta\,|01\rangle + \sqrt{\frac{1}{6}}\beta\,|10\rangle \tag{14}$$

$$|\chi_1\rangle = \sqrt{\frac{2}{3}}\beta|11\rangle + \sqrt{\frac{1}{3}}\alpha|\Phi_+\rangle = \sqrt{\frac{2}{3}}\beta\,|11\rangle + \sqrt{\frac{1}{6}}\alpha\,|01\rangle + \sqrt{\frac{1}{6}}\alpha\,|10\rangle \tag{15}$$

2.3 Single state fidelity

$$|\Psi\rangle = |\chi_0\rangle|0\rangle + |\chi_1\rangle|1\rangle = \left(\sqrt{\frac{2}{3}}\alpha|00\rangle + \sqrt{\frac{1}{3}}\beta|\Phi_+\rangle\right)|0\rangle + \left(\sqrt{\frac{2}{3}}\beta|11\rangle + \sqrt{\frac{1}{3}}\alpha|\Phi_+\rangle\right)|1\rangle$$

$$\rho_{a_0,a_1} = \mathrm{Tr}_{b_1}[|\psi_4\rangle\langle\psi_4|] = |\chi_0\rangle\langle\chi_0| + |\chi_1\rangle\langle\chi_1| =$$

Note that both $|\chi_0\rangle$ and $|\chi_1\rangle$ are invariant under exchange of the qubits. This implies that $\rho_{a_0} = \rho_{a_1}$, i.e. the copies are identical (there is no different in calculating the partial trace in one Hilbert space or the other). Hence:

$$\begin{aligned}
\rho_{a_0} &= \mathrm{Tr}_{a_1}[|\chi_0\rangle\langle\chi_0| + |\chi_1\rangle\langle\chi_1|] = \mathrm{Tr}_{a_1}[|\chi_0\rangle\langle\chi_0|] + \mathrm{Tr}_{a_1}[|\chi_1\rangle\langle\chi_1|] = \\
&= \frac{2}{3}|\alpha|^2|0\rangle\langle 0| + \frac{1}{6}|\beta|^2|0\rangle\langle 0| + \frac{1}{6}|\beta|^2|1\rangle\langle 1| + \frac{1}{3}\alpha\beta^*|0\rangle\langle 1| + \frac{1}{3}\alpha^*\beta|1\rangle\langle 0| + \\
&+ \frac{2}{3}|\beta|^2|1\rangle\langle 1| + \frac{1}{6}|\alpha|^2|0\rangle\langle 0| + \frac{1}{6}|\alpha|^2|1\rangle\langle 1| + \frac{1}{3}\alpha\beta^*|0\rangle\langle 1| + \frac{1}{3}\alpha^*\beta|1\rangle\langle 0| = \\
&= \frac{5}{6}|\alpha|^2|0\rangle\langle 0| + \frac{5}{6}|\beta|^2|1\rangle\langle 1| + \frac{1}{6}|\beta|^2|0\rangle\langle 0| + \frac{1}{6}|\alpha|^2|1\rangle\langle 1| + \frac{2}{3}\alpha\beta^*|0\rangle\langle 1| + \frac{2}{3}\alpha^*\beta|1\rangle\langle 0| = \\
&= \frac{5}{6}|\alpha|^2|0\rangle\langle 0| + \frac{5}{6}|\beta|^2|1\rangle\langle 1| + \frac{5}{6}\alpha\beta^*|0\rangle\langle 1| + \frac{5}{6}\alpha^*\beta|1\rangle\langle 0| - \\
&- \frac{1}{6}\alpha\beta^*|0\rangle\langle 1| - \frac{1}{6}\alpha^*\beta|1\rangle\langle 0| + \frac{1}{6}|\beta|^2|0\rangle\langle 0| + \frac{1}{6}|\alpha|^2|1\rangle\langle 1| = \\
&= \frac{5}{6}|\psi\rangle\langle\psi| + \frac{1}{6}|\psi_\perp\rangle\langle\psi_\perp|,
\end{aligned}$$

where $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is the input state and $|\psi_\perp\rangle = \beta^*|0\rangle - \alpha^*|1\rangle$ is its orthogonal state.

A common figure of merit used in order to estimate the closeness of two quantum states is the fidelity [Ref: Nielsen and Chuang]

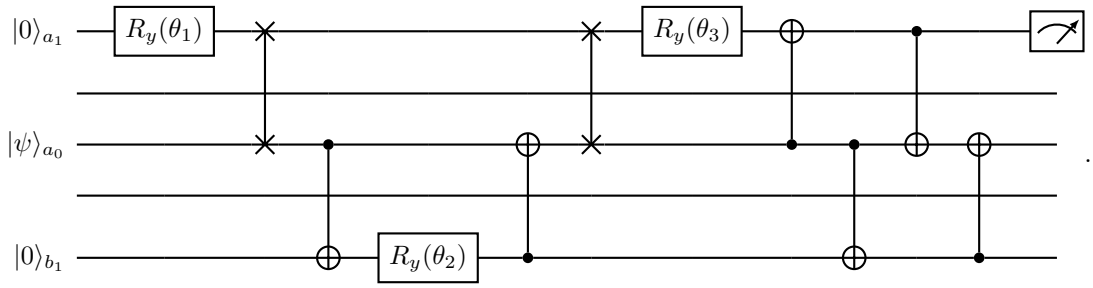
$$F(|\psi\rangle, \rho) = \langle\psi|\rho|\psi\rangle \tag{16}$$

In our case, the fidelity of the output copies is:

$$F(|\psi\rangle, \rho_{a_0}) = \langle\psi|\rho_{a_0}|\psi\rangle = \frac{5}{6} = F(|\psi\rangle, \rho_{a_1})$$

3 Implementation of UQCM in QI

In order to run the circuit on Starmon-5, we have to consider that we can only apply 2-qubits gate on nearest neighbours. In order to overcome this problem, we have introduced two SWAP gates (this is not the best choice probably, it can be done with only one).



The generic input state $|\psi\rangle$ can be prepared from $|0\rangle$ performing two rotations:

$$|\psi\rangle_{a_0} = R_z(\phi)R_y(\theta)\,|0\rangle$$

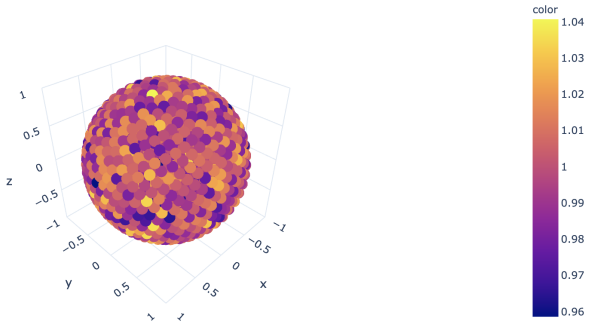
The final measurement is performed in the $\{|\psi\rangle\,, |\psi_\perp\rangle\}$ basis. The probability of getting $+1$ as outcome is:

$$p_{+1} = \mathrm{Tr}[|\psi\rangle\langle\psi|\,\rho_{a_1}] = \langle\psi|\,\rho_{a_1}\,|\psi\rangle = F(|\psi\rangle\,, \rho_{a_1}).$$

Hence, we can measure the fidelity directly, without having to perform a quantum tomography experiment. In order to perform this measurement, we implement the inverse rotations with respect to the ones used to prepare the input state. Hence, we first rotate with $R_z(-\phi)$ and then with $R_y(-\theta)$. We conclude by measuring in the computational basis.

QXSimulator

In order to verify that our implementation of the AQCM is correct, we first ran the experiment on the QXSimulator, considering 1000 points on the Bloch sphere and 1024 shots for each point. NB: In the following pictures $F_{measured}/F_{optimal}$ is plotted.




```
Number of points:  1000
Average fidelity:  0.833333984375
Standard deviation:  0.011917361703802065
```

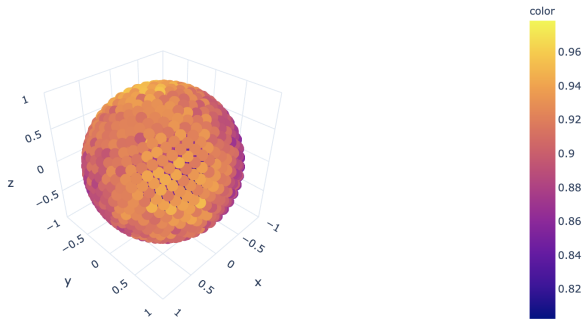
When averaging over the Bloch sphere, we obtain

$$\overline{F} = 0.833 \pm 0.011.$$

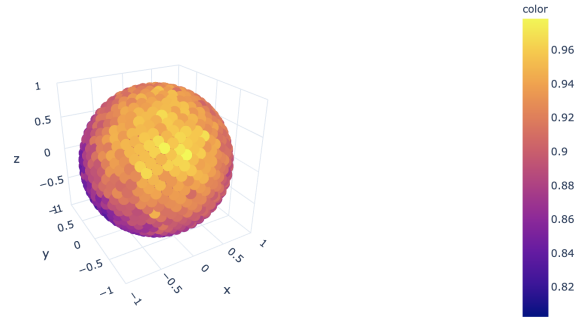
This is consistent with the expected value $F_{optimal} = \frac{5}{6} = 0.833\ldots$

Starmon-5

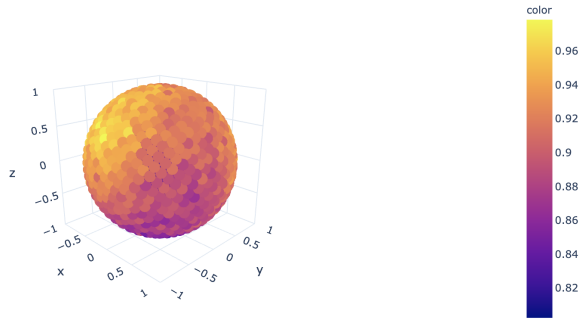
Afterwards, we ran the circuit on Starmon-5. We sampled the Bloch sphere using 1000 points and considering 4096 shot for each point. NB: In the following pictures $F_{measured}/F_{optimal}$ is plotted.



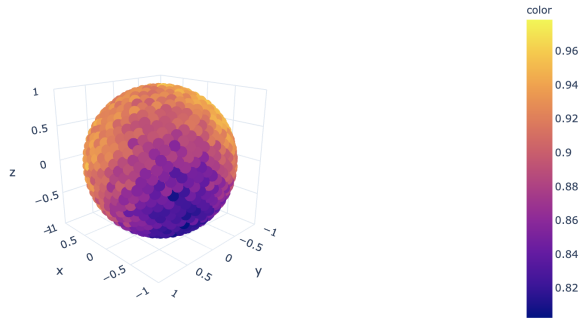

```
Number of points:  1000
Average fidelity:  0.745986328125
Standard deviation:  0.03161861869451461
```




```
Number of points:  1000
Average fidelity:  0.745986328125
Standard deviation:  0.03161861869451461
```




```
Number of points:  1000
Average fidelity:  0.745986328125
Standard deviation:  0.03161861869451461
```




```
Number of points:  1000
Average fidelity:  0.745986328125
Standard deviation:  0.03161861869451461
```

When averaging over the Bloch sphere, we obtain

$$\overline{F} = 0.75 \pm 0.03.$$

As expected, this is lower than the optimal fidelity. When running on real hardware, noise will reduce the quality of the copies.

4 Simulation of QKD Attack by a eavesdrpper equipped with UQCM

In this section we investigate whether we can attack QKD protocol equipped with a UQCM. We briefly review the BB84 QKD protocol[**?**]

1. Bob randomly picks a basis $B_i \in \{X, Z\}$ and randomly picks a private bistring $b_i \in \{0, 1\}$.

2. Bob prepare the qubit in state in $|0\rangle, \text{or } |1\rangle \text{ or } |+\rangle, \text{or } |-\rangle$ depends on what basis and key he got.

3. Bob sends his qubit to Alice.

4. Alice measure the qubit in a random picked basis $\tilde{B}_i \in \{X, Z\}$.

5. The above process is repeated for several times to send a multiqubit key.

6. Bob and Alice publish their measurement basis.

7. Compare the basis and drop the measurement result with different basis.

8. Check result for part of the measurement with same basis (in public channel). If the error rate is above threshold, abort the process (for possible eavesdrping or noise).

9. Preserve all remained measurement and take the result as a key.

4.1 Intercept and resend Attack

Suppose Eve eavesdrping by intercepting and randomly measuring the qubit, then resending a new one based on his measurement result. The probability of Eve being detected for a single qubit is $\epsilon = 1/4$.

If the remained bitstring is of length k, Bob and Alice will preserve $k/2$ bits for error check, then probability of a successful eveasdroping without being noticed is

$$P(k) = (1-\epsilon)^{k/2}$$

For a lone key with more than 10^2 bits, a brief estimation under ideal condition is given by

$$P \approx 10^{-12}$$

theoretically it's almost impossible to eveasdroping without being detected.

However, the near-term quantum device is always noisy, which means error is possible when Bob and Alice compare their qubits. That's why we need a threshold m to allow some extent of error tolerance,

$$P(k,p) = \sum_{j=0}^{m} \binom{k/2}{m} \epsilon^j (1-\epsilon)^{k/2-j}$$

The threshold p should depends on the fidelity of the quantum channel in which Alice and Bob transfer their qubits.

Consider a channel single-bit depolarizing noise characterized by p

$$\mathcal{D}_p : \rho \to p\rho + (1-p)\mathbb{1}/2$$

Then the probability of get a bit filp for single qubit is $\epsilon' = (1-p)/2$.

Then we can derive the flip probability of a single bit

$$\epsilon'' = (1-\epsilon)\frac{1-p}{2} + \epsilon\frac{1+p}{2} = \frac{1}{2}(1-p+2p\epsilon)$$

When the net error reach the same level with the environment noise, we can say that error introduced by Eve can't be distinguished.

4.2 Attack with Quantum Copying Machine and Quantum Memory

Assuming Eve has a quantum copying machine and a quantum memory capable to store all the qubits intercepted, then the eveasdroper can partially clone and store all the qubits, then measure them after Alice and Bob publish their measurement basis.

The maximum fidelity of UQCM is $F = 5/6$. Thus the minimum error rate of a single qubit is $\epsilon = 1/6$.

The success rate of Eve still decays exponentially with key length, but with a lower rate. For a lone key with more than 10^2 bits, apply the same formula we get

$$P \approx 10^{-9}$$

The successful probability has been raised by 10^3 times, but still unrealistic.