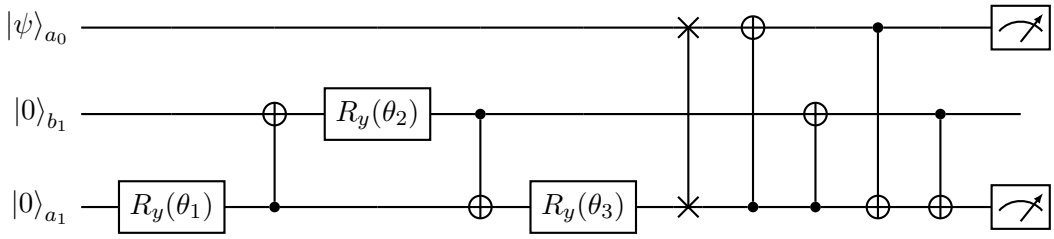
Quantum project: Report 2

December 8, 2020

1 Report 2

1.1 Updated circuit

We updated the circuit considering only 1 SWAP gate:



This is also how IBM transpiles the original circuit proposed in [Ref Buzek-Hillery] in order to run it with only nearest neighbour couplings.

We are now measuring both the copies. We are checking whether the QCM is actually symmetric.

1.2 Results on Starmon

See Jupyter.

1.3 Results on IBM

See Jupyter. We turned off the optimization in the transpiling process. The transpiler only adds the SWAP gate in order to allow the circuit to run when only nearest neighbour coupling are allowed (usually it is not possible to have three qubits reciprocally connected). When using the Yorktown backend, no SWAP gate is necessary.

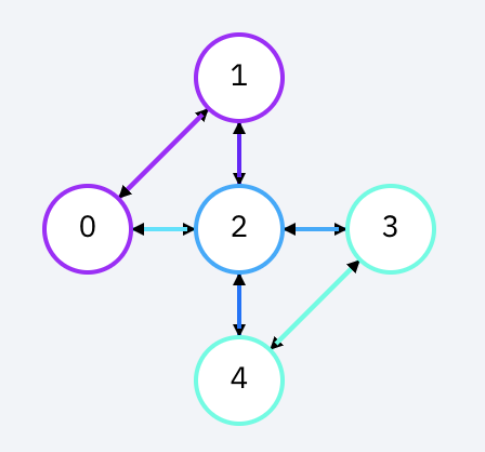


Figure 1: Connectivity of Yorktown IBM device.

1.4 Comparison

	Starmon 5	**Athens**	**Ourense**	**Santiago**	**Valencia**	**Vigo**	**Yorktown**
F_1	0.73	0.77	0.78	0.73	0.6	0.76	0.76
σ_{F_1}	0.03	0.02	0.03	0.04	0.2	0.03	0.02
F_2	0.73	0.78	0.72	0.72	0.6	0.75	0.76
σ_{F_2}	0.05	0.02	0.03	0.04	0.2	0.03	0.02
F_2/F_1	1.00	1.01	0.93	0.98	1.1	0.99	1.00
σ_{F_2/F_1}	0.04	0.03	0.03	0.03	0.7	0.02	0.03

1.5 Readout calibration

We considered that a classical error can affect the measurement process. Consider a state of the form $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$. The expectation value of a measurement along the Z axis is given by $\bar{m} = p_{+1} - p_{-1}$. However, this quantity can be affected by classical errors, such that it is transformed to,

$$\begin{aligned} \bar{m} &= (1-2\epsilon_{10})|\alpha|^2 - (1-2\epsilon_{01})|\beta|^2 && (1)\\ &= (\epsilon_{01}-\epsilon_{10}) + (1-\epsilon_{01}-\epsilon_{10})(|\alpha|^2 - |\beta|^2) && (2)\\ &= \beta_0 + \beta_1\langle Z\rangle. && (3) \end{aligned}$$

Note that $|\alpha|^2 = p_{+1}$ and $|\beta|^2 = p_{-1}$. Then, we can find the corrected expectation value as,

$$\langle Z\rangle = \frac{\bar{m}-\beta_0}{\beta_1}. \quad (4)$$

The parameters β_0 and β_1 can be estimated from experimental measurements of eigenstates of the Z basis, that is, $|0\rangle$ and $|1\rangle$. Then, they can be used to correct the outcome of future experiments, for example a quantum state tomography. In Fig. 1.5 one can observe a check that the results have been calibrated. It corresponds to the average Z value of a single qubit, when it is rotated along the X axis from 0 to 2π. The blue curve represents the measurement outcomes without any correction, while the orange curve represents the corrected measurements.

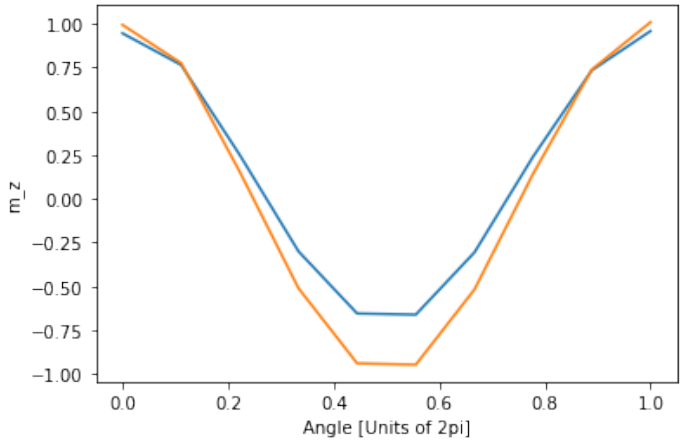


Figure 2: Calibration check on qubit 0 of Starmon five. The calibration parameters were estimated to be $\beta_0 = 0.1229$ and $\beta_1 = 0.8278$. Blue curve corresponds to the pure results. Orange curve corresponds to the corrected results.

We are not only interested in corrected the expectation value, but also the coefficients associated to each measurement outcome. For such purpose, we consider corrected coefficients $p\tilde{}_{+1}$ and $p\tilde{}_{-1}$ that satisfy the following equations,

$$\begin{cases} p\tilde{}_{+1} + p\tilde{}_{-1} = 1 \\ p\tilde{}_{+1} - p\tilde{}_{-1} = \frac{\bar{m}-\beta_0}{\beta_1} \end{cases} \tag{5}$$

By solving this system of equations, we find that the corrected coefficients are given by

$$p\tilde{}_{+1} = \frac{\beta_1 - \beta_0 + p_{+1} - p_{-1}}{2\beta_1}, \qquad p\tilde{}_{-1} = \frac{\beta_1 + \beta_0 - p_{+1} + p_{-1}}{2\beta_1}. \tag{6}$$

From this parameters we can correct the previous results corresponding to the average fidelity of the quantum copy machine on the Bloch sphere.

2 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.

2.1 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 eavesdroping 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.

2.2 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 eavesdroper 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

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

3 Error Rate in Noisy Reality

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

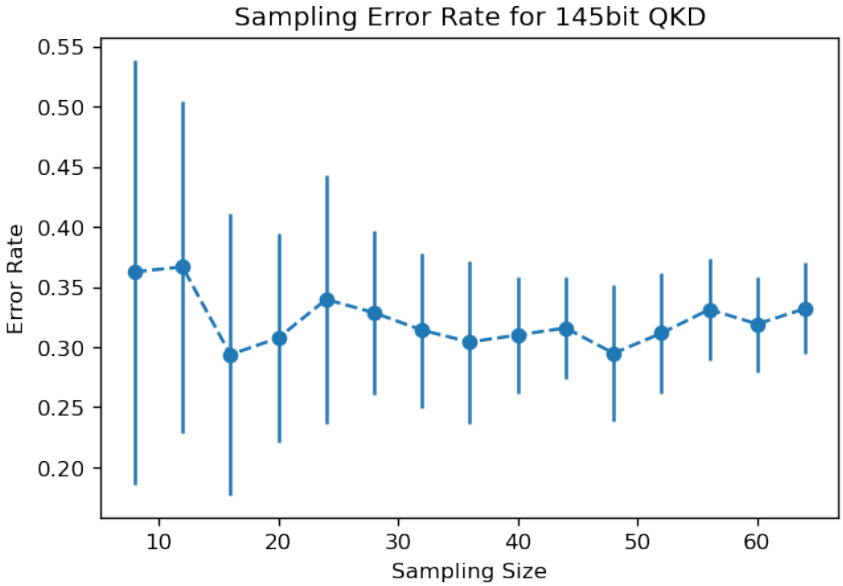


Figure 3: Sampling Error for 144bit QKD

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.

If Alice and Bob use a random sampling check to avoid eavesdrppor, suppose the sampling size is N, then the average error rate is defined as

$$\delta = \frac{|\{x_i | x_i^A \neq x_i^B\}|}{|\{x_i\}|}$$

The average error rate only relys on the noise of our quantum hardware, it's not related with key length or sampling size.

The average result we obtained is

$$\delta = (0.32463 \pm 0.02097)$$

We simulate a single-shot QKD process on Starmon-5, with 64, 128 and 144 key length. A example table is shown as

No.	Key	Measure Basis	Bob	Eve
0	0	Z	1	0
1	1	X	1	0
2	0	X	0	1
3	1	X	1	1
4	0	Z	0	0
5	0	X	0	1
6	0	Z	1	1
7	0	Z	1	0
8	0	X	0	0
9	0	Z	0	0
10	0	Z	0	0
11	1	X	0	1
12	1	X	1	1
13	1	Z	1	1
14	0	X	0	1
15	0	Z	0	1
16	1	X	1	1
17	1	X	1	0
18	0	Z	0	0
19	1	Z	0	0
20	0	X	1	1
21	1	Z	0	0
22	1	X	0	0
23	1	Z	1	1
24	1	Z	1	1
25	0	X	0	1
26	1	X	0	0
27	0	Z	0	1
28	0	Z	1	1
29	1	X	1	0

Where the measurements with different basis are ignored, the measurement basis here is the common basis for Alice and Bob.

3.1 Next meetings

1. Readout correction on IBM
2. Readout correction for all the five qubits of starmon.
3. Phase covariant cloning machine (optimal copy of the states on one equator)
4. Economical cloning machine (2 qubits, we could run it on Spin-2!)
5. Asymmetric Fourier cloning machine (?)