Quantum project: Report 3

December 8, 2020

1 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 $|0\rangle$, or $|1\rangle$ or $|+\rangle$, 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. Sampling the remained measurement, check the result(in public channel). If the error rate is above threshold, abort the distribution process (for possible eavesdrping).
9. Preserve all remained measurement and take the result as a key.

1.1 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.

1.2 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

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

2 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 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

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

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

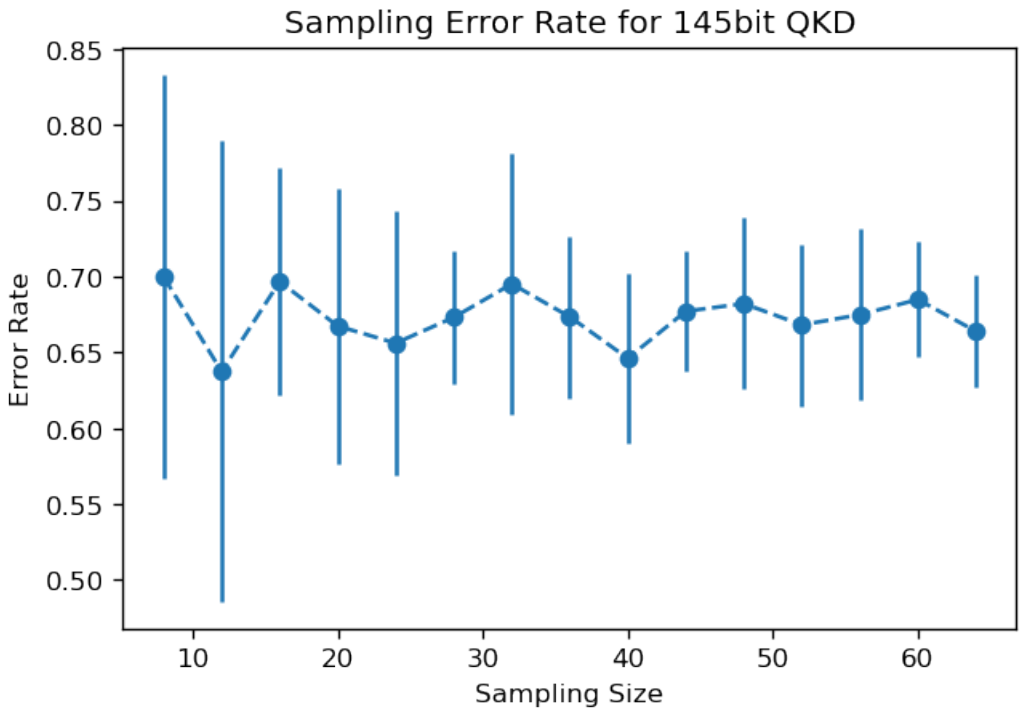

Figure 1: Sampling Error for 144bit QKD

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

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

$$\delta = (0.67774 \pm 0.02140)$$