Quantum Key Distribution by Drone

Z. Wang, Z. Guo, G. Mogos* and Z. Gao

Department of Computing, School of Advanced Technology, Xi’an Jiaotong-Liverpool University, Suzhou, China

*Corresponding author email: Gabriela.Mogos@xjtlu.edu.cn

Abstract. A cryptographic communication system is secure from a practical point of view if the encryption scheme can be broken after X years, where X is determined by security needs and existing technology. Quantum cryptography does not offer a complete solution for all cryptographic problems: secure keys, encryption algorithms based on them, message authentication and finding ways to detect / prevent interception; but it can be seen as a complement to standard symmetric cryptographic systems. This paper presents the implementation of the BB84 quantum key distribution protocol on mobile systems - Amov-lab's Z410 drone with T-engine 2216 - and tracks the error rate obtained in flight conditions.

Keywords: Qubit; Drone; BB84 protocol.

1. Introduction

The advantage of quantum cryptography is that it offers, instead, a quantum key distribution / exchange procedure that can automatically detect if communication interception occurs. The security of sending messages implies not only the existence of secure keys, but also the security of the other procedures mentioned above (encryption algorithms, authentication).

Due to the fact that qubits observe the laws of quantum physics, they can provide a secure basis for the exchange of secret messages. In the experimental realizations of quantum cryptography, qubits are generally photons, whose polarization state or phase encodes logic states 0 or 1. Such qubits that can be easily generated and that are transportable by optical fibers are very useful in secret communications because the parts that communicate can have a code that cannot be broken, if they share a newly created identical sequences of random bits, called one-time pad codes.

The paper presents the first results of the implementation of Bennett - Brassard BB84 quantum key distribution protocol on mobile devices. The mobile device used in our project is an Amov-lab's Z410 drone with T-engine 2216 and Pixhawk flight control, additionally equipped with a raspberry pi. In our project we considered that the key exchange is done in the absence of an intruder and we followed the error rate obtained in flight conditions.

2. BB84 Quantum Key Distribution Protocol

Quantum cryptography is a combination between quantum physics and the art of encoding. For the first time, the idea of quantum cryptography was introduced in an unpublished manuscript by Stephen Wiesner in 1970 and was presented by Bennett and Brassard in 1984 [4], becoming a subject of interest. Quantum cryptography uses quantum physics properties like the no-cloning theorem, the Heisenberg uncertainty principle, and irreversibility of quantum measurements to ensure the security of its methods. Charles Bennett from IBM together with Gilles Brassard from the University of Montreal (1984 - 1985) developed a key distribution protocol using polarized photons to codify the information. The symmetric
Bennett - Brassard protocol (BB84) [4] bases its security on physical laws (of quantum physics) rather than on mathematical complexities, and therefore its security is independent of possible advances in computational techniques. The problem of securely exchanging random bit sequences is identical to the original problem of exchanging meaningful messages in a secure way. With the help of quantum physics such a secure exchange is possible only if the bit sequence is random.

The quantum key distribution QKD protocol BB84 consists of: Alice sends Bob a long sequence of qubits in the form of randomly polarized photons in one of four possible states: (the Dirac notation is used)

1) horizontal linear polarization (state $|0\rangle$),
2) vertical linear polarization (state $|1\rangle$),
3) diagonal polarization at $\pi/4$ compared to the vertical (state $H|0\rangle$, obtained by applying the Hadamard gate $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ on state $|0\rangle$),
4) diagonal polarization at $-\pi/4$ compared to the vertical (state $H|1\rangle$, obtained by applying the Hadamard gate $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ on state $|1\rangle$).

The first two states form the horizontal-vertical base, and the last two states form the diagonal polarization base. These are two orthonormal bases with which the polarization state of a photon can be completely described.

For each photon, Alice randomly chooses a type of polarization (horizontal-vertical or diagonal) and within each type randomly chooses a value of polarization (one of the two orthogonal states associated with that type of polarization. In formal language, the four types of qubits equally probable sent by Alice to Bob can fall into two categories: states $|0\rangle$ and $|1\rangle$ form qubits type-S (standard), and states $H|0\rangle$ and $H|1\rangle$ form qubits type-H.

Observations / measurements based on type-S are incompatible with measurements based on type-H; that is why two bases are used.

As he receives a qubit, Bob randomly decides whether to send it directly to a measuring gate or apply a Hadamard gate to it before measuring it. These two options represent, respectively, S-type and H-type measurements.

Qubits should be individually identifiable (for example, by the order in which they arrive), so that Bob and Alice can correctly identify them and compare information about them.

After Bob measures his qubits, Alice communicates to him through an unsecured channel which qubit is S-type, and which is H-type but does not tell him in which of the two states she prepared the qubits. For those qubits for whom Bob's random choice of the type of measurement is in agreement with Alice's random choice of the type of qubits she sends, Bob finds out from the result of his measurement what is the randomly selected value (0 or 1) sent by Alice.

Finally, Bob transmits to Alice, through an insecure channel, which of the qubits he subjected to a certain type of measurement coincides with her choice regarding the type to prepare them, i.e. which qubits gives them identical random bits. They ignore the other qubits and are thus able to build single-use protected codes from the identical sequence of random bits they obtained.

The reason Alice and Bob have to give up half of the qubits is the security against intercepting communication. If Alice sent all qubits of the same type and Bob always made the same type of measurements and always got a bit that matched Alice's (or if Alice sent with each qubit the classic information about his type), an intruder (Eva) could intercept the same information as Bob without being detected.

Our project aims to transmit encrypted images obtained with a mobile drone device. We have used a symmetric cryptosystem where the encryption/decryption key is obtained with the Bennett-Brassard BB84 quantum key distribution protocol.

3. Implementation on Mobile Device

For the encrypted transmission of the images, we used an Amov - lab's Z410 drone with T-engine 2216 and Pixhawk flight control, additionally equipped with a raspberry pi 3B + and a video camera.
In our project the key exchange is between the drone and a laptop on the ground. The protocol is initialized by the drone after it takes an in-flight image. In the key distribution protocol, the drone is the sender, and the laptop is the receiver.

The laptop performs the following tasks:
- provides GUI to the user.
- receives qubits from raspberry pi (plays the receiver role).
- exchanges basis with the raspberry.

The quantum key distribution protocol is implemented in python [4] using QTDesigner to build the GUI interface. The MAVLink protocol [1] for communicating with drones is used.

The raspberry pi [3] performs the following tasks:
- commands the flight controller. There is used an open-source autopilot system - the PX4 autopilot [2].
- initiates key exchange and image encryption.
- sends qubits to the laptop (plays the sender’s role in the BB84 protocol).
4. Results
A series of tests were performed for different sender-receiver distance and for different input data (number of qubits).
The tests tracked the error rate obtained by the quantum key distribution protocol in flight conditions. The error rate obtained for different lengths of qubit string is measured when the sender-receiver distance varied (see table 1), always the receiver being located on the ground.
Thus, the input data (number of qubits) has varied from 100 to 1000 and the sender-receiver distance from 0 - 40 meters.

Table 1. Results.

| Qubits string | 0 m | 5 m | 10 m | 15 m | 20 m | 25 m | 30 m | 40 m |
|---------------|-----|-----|------|------|------|------|------|------|
| Length 100    | 0.0%| 46.0%| 52.0%| 56.0%| 59.0%| 64.0%| 68.0%| 72.0%|
| Length 200    | 25.0%| 62.5%| 69.5%| 74.5%| 79.5%| 84.5%| 89.5%| 94.5%|
| Length 300    | 45.0%| 75.0%| 82.5%| 89.0%| 95.0%| 99.0%| 99.0%| 99.0%|
| Length 400    | 65.0%| 95.0%| 100% | 100% | 100% | 100% | 100% | 100% |

Table 1 shows that, the error rate is around 50%, respecting the theoretical model, the additional errors introduced by the equipment are not significant.
We performed 3 tests following the error rate obtained on the same parameters (input data and sender-receiver distance). These are shown in the chart below (figure 4).
The first test shows peaks (slight increases) in error rate values of more than 55%.
These increases in errors can be considered to be due to the equipment, given that during the experiment we used an isolated network (no intruders).
5. **Conclusion**

In quantum cryptography, two communication channels are used: a unidirectional quantum channel (through which Alice sends qubits to Bob), and a public bi-directional channel, which can also be heard by an intruder (Eva).

If the transmission channel introduces a high error rate, the receiver (Bob) cannot distinguish between errors caused by noise (for example, not receiving a qubit due to transmission or detection errors) and those due to interception by an intruder (Eva); that is why the receiver assumes that all the errors are due to an intruder (Eve) and in this sense a communication key is only partially secured.

These results represent QKD’s first steps towards implementation in mobile devices and IoT. Even though the error rate is relatively high, using such encryption can increase the security of the distributed key. For symmetric cryptosystems, methods to obtain the encryption key based on the laws of quantum physics have proven to be secure compared to classical keys.

**References**

[1] https://mavlink.io/en/
[2] https://px4.io/
[3] https://dojofordrones.com/raspberry-pi-drone/
[4] https://dronekit-python.readthedocs.io/en
[5] Bennett, C. and Brassard, G. 1984. *Quantum cryptography: Public key distribution and coin tossing*, Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing 175.