ISSN (e): 2250 – 3005 || Volume, 14 || Issue, 6|| Nov. - Dec. –2024 ||
International Journal of Computational Engineering Research (IJCER)

An inexpensive and convenient replacement alternative solution for quantum key distribution based security systems

Catalin Silviu Nutu
Constanta Maritime University, Mircea cel Batran Bd. 104, Constanta, Romania

Abstract. *The quantum key distribution (QKD) technology exhibits in the present a series of weaknesses and shortcomings which make it rather hard to be implemented and used on a large scale. Some of these issues and limitations are presented in the first section of the paper.This paper proposes a replacement solution for a QKD based security systems. This solution uses a circuit which generates a square wave signal of ever increasing duration. The duration of the increasing square wave pulses can be modified by adjusting the values of two resistors R_2 and R_4 as well as by adjusting the value of the capacitor C_2 taking values within the intervals specified in the wiring diagram. The encrypted communication is ensured by the use of two distinct identical such circuits, which have the values of R_2, R_4 and C_2 set on the very same values. The generation of the encryption key used in the secret communication, is explained in the paper. This circuit related to the proposed solution has been constructed by the author and it can be seen working in the YouTube video referenced. This hardware can be further expanded in the way it is explained and described in this paper, and such an expanded solution can also be automated using robots and AI instead of being operated by persons. The features and both the upsides and downsides of the solution proposed are also presented in the paper.*

Keywords. *Quantum key distribution (QKD), encryption, communication, ever increasing square wave signal*

Date of Submission: 26-11-2024 Date of acceptance: 05-12-2024

I. Quantum key distribution security systems

Quantum key distribution (QKD) based security systems are nowadays very fashionable and in trend, as a modern and fancy solution for encrypting and thus ensuring a secret communication channel.

These QKD based security systems, however, exhibit at their present stage, a series of weaknesses, disadvantages, issues and limitations which make them in the present not so trustworthy and not so desirable, despite the fact that their name sounds so appealing.

Some of the most significant among these issues, limitations, weaknesses and disadvantages of the QKD systems are:

- They cannot be implemented in software or as a service on a network, and cannot be easily integrated into existing network equipment. Since QKD is hardware-based it also lacks flexibility for upgrades or security patches
- They are very expensive to implement on a scale
- The technology is practically still not here yet
- Photon polarization might be impacted in the traveling medium
- Quantum storage issues: Developing reliable quantum memory that can store quantum states long enough for practical communication applications is still a challenge.
- They can only be used in short distances. Quantum communication is currently limited by how far qubits can be sent without degradation, known as the "range problem." In quantum cryptography, a key issue is the limit on sharing keys over long distances. Quantum systems face challenges like photon loss and decoherence, making long-distance communication tough. Thus, sending secure keys becomes harder with distance
- Due to their fragility, qubit interconnection, decoherence, and external noise, quantum systems are prone to errors

- QKD has provable security based on information theory, and forward secrecy. The main drawback of quantum-key distribution is that it usually relies on having an authenticated classical channel of communication
- Compared with standard computers, quantum computers are extremely susceptible to noise. The quantum state of qubits is extremely fragile and any disturbance, such as a slight vibration or a change in temperature, can uncontrollably affect the computer, causing information stored to be lost.
- One major challenge to widespread quantum computing adoption is the qubit's fragile state. Quantum computers encode information into qubits using ions, light or magnetic fields. Existing technologies can only keep the information in a quantum state for brief periods, limiting the duration of calculations

II. QKD replacement security system

2.1 Presentation of the hardware used for QKD replacement security system

Taking into account all the issues, limitations, weaknesses and disadvantages of the QKD systems presented above, this paper proposes an inexpensive and convenient replacement alternative solution, in order to overcome a great deal of the issues and limitations of the QKD system, presented in the previous section of this paper.

The wiring diagram presented in Figure 1 below, represents a circuit which generates an ever increasing duration of the square wave pulses and it can be successfully used to generate a replacement alternative solution for the QKD encrypted communication between Bob and Alice.

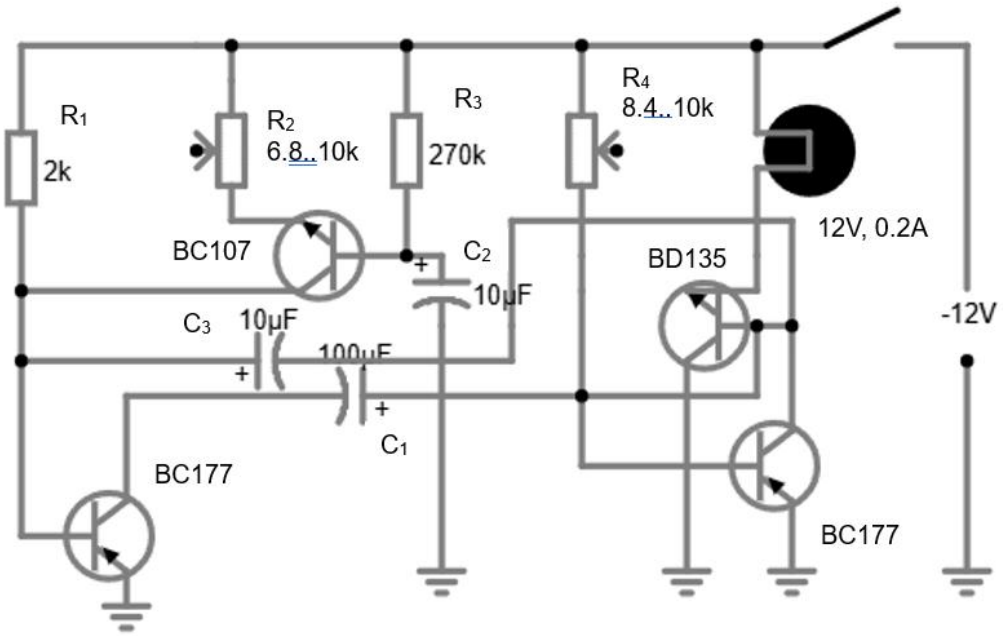

Figure 1. Wiring diagram of the device used to replace QKD encrypted communication

The actual functioning of this circuit above, also physically built by the author, is explained by the author in one of his YouTube videos, explaining the construction of this device used to generate encrypted communication, which can be visited using the link provided in [4] in the References. The capacitor C_2in the wiring diagram may be also a variable capacitor, to take values of capacitance between 4.7 and 10 uF.

By adjusting the values of R_2, R_4 and C_2, using potentiometers and variable capacitors instead of fix value resistors and fix value capacitor, one can easily modify the duration of the square wave pulses, represented by the time periods when the bulb lights up.

However, in order to use this circuit for the purpose intended in this paper, at the bulb's terminals in the wiring diagram, an oscilloscope should be also connected, in order to measure the exact duration of the square wave pulses, since the encryption of the communication between Bob and Alice is based on the duration of these square wave pulses.

In order that the encrypted communication between Bob and Alice is ensured, they both have to have two distinct identical circuits built in accordance with the wiring diagram above.

This is absolutely necessary, because the square wave pulses generated by means of the circuits also have to be identical for a smooth and exact communication, since the encryption keys used in the

communication between Bob and Alice depend on the shape of the signal generated with the circuit, this is to say they depend on the duration of the square wave signal, as it is explained in this paper.

2.2 Procedure used for the encrypted communication

Let us now see and understand how the proposed encryption communication system works:

- Bob and Alice set the same values forR_2, R_4 and C_2, so that under the assumption that both hardware is identical in construction and functioning, they will both produce the same square wave signal
- Bob and Alice agree upon a set of encryption rules to generate the encryption key used in their communication at a certain time.Namely, they choose a string with k terms, where k is the number of pulses of the square wave signal and they assign for a certain duration of a square wave pulse, the value 0 or 1
- The encryption key is thus generated for each shape of the square wave signal and the encrypted communication can take place using the secure key generated in the manner presented above

III. Extensionsof the hardware and possible automations to beused to improve the proposed QKD replacement system

One of the improvements of the system presented may be achieved by designing and building of a circuit able to generate not only anever increasing square wave pulses but square wave pulses of variable duration. This can be made using as core component an integrated circuit, able to do this task.

Another improvement of the hardware is to increase the number of variable dipolar elements, e.g. to use instead of R_2, three variable parallel connected resistors R_{21}, R_{22} and $R_{23\ of}$ 30kOhms each, four variable parallel connected resistors R_{41}, R_{42}, $R_{43\ and}$ R_{44} of 40kOhms each, and three series connectedcapacitors instead of the single one.

The square wave signal will depend, in this case of many more variable components and this makes the communication between Bob and Alice a lot harder to be hacked.

In order to improve security, one can also use an additional encryption level when transmitting the values of the variable components used, e.g. A=30.0kOhms, B=30.1kOhms, etc.

Other improvements which can be made regard the automation of the entire encrypted communication and its related encryption/ decryption process, thus rendering Alice and Bob useless. This can be achieved by using A.I. computer subroutines, robots to set values of potentiometers and of variable capacitors, automated systems to encrypt/ decrypt the messages, but also automated communication between parties.

The first step in the automation subroutine is that the robots taking the tasks of Alice and Bob, set the values of potentiometers and of variable capacitors used in the hardware.

The square wave signal is then read from the oscilloscope which is robot inbuilt in both of the robots used in the one to one communication.

Depending on the shape of the square wave signal, and depending on the encryption rules assigned and used, the encryption key used in the secure communication follows: [0, 1, 1, 0, …].

The encryption key, as resulted before, is used to encrypt communication and thus to securely communicate.

IV. Features, strengths, issues and weaknesses of the QKD replacement security system

The alternative solution for QKD secured communication proposed by this paper and the hardware related to this solution, is a much more inexpensive technology to use, than the QKD technology. By contrast with the QKD technology, it can be used over long distances, provided that the communication line is secure, but also encrypted, out of security reasons.

The proposed replacement system can be more easily implemented in practice than the QKD based security systems.

The use of the presented system does not require huge amounts of memory, such as in the case of QKD based security systems.

The replacement system presented is stable in comparison with the high instability exhibited by the QKB based security systems.

One of the strengths of this replacement system which is also exhibited by the QKD based security systems, that makes this system hard to be broken, is the variable number of bits depending on the number of square wave pulses, which is used for the encryption key.

The number of bits depends on the shape of the signal generated, by means of the number of square wave pulses available for a certain combination of the variable components' values, andthus depends on the values set for the variable components of the resistors and capacitors used in the hardware.

The proposed QKD replacement system exhibits,however, also a series of issues and weaknesses, some of them also to be encountered when using QKD encrypted communication.

One of these common issues is to ensure the secure communication of the values of R_2, R_4 and C_2 between Alice and Bob.This is also an issue of QKD systems, wherethe related classical communication is also used when communicating overthe QKD security systems.
Another issue to be taken into consideration is the secrecy regarding the construction of the hardware, that is to say the construction of the square wave pulse generator. Its construction can be made more complex, in order to give additional strength for the security of communication, as it is presented in the section above.
A third issue to be dealt with is the calibration of the hardware used in communication and to ensure that both hardware is identical in construction and functioning, and hence, that they generate the same square wave signal, for a certain set of values chosen for the parametric variable components.
A fourth weakness and security issue of the system presented is related to the automation of the respective system. However, this is an issue which is always present when dealing with every piece which embeds smart technology.
When automating the system presented,and when robots set the values of variable components of the hardware, the technology thus used introduces its own vulnerabilities in the respective communication system.
This is because any robotor any smart technology is prone to cyber attacks according to the principle "if a technology is smart than it is vulnerable to attacks".
That is why, by using persons to operate the setting of the values of variable components, the security of the communication may be actually better, under the assumption that those persons are loyal to their employers.

V. Conclusions

The replacement alternative solution proposed by this paper can successfully replace a QKD security system, being able to overcome many of the weaknesses and issues of the QKD based security systems.
One of its main advantages is that it is a much more inexpensive technology to use, than the QKD technology.
By contrast with the QKD technology, it can be used over long distances, provided that the communication line is secure, and also encrypted, out of security reasons.
The proposed replacement system can be more easily implemented in practice than the QKD based security systems.
The use of the presented system does not require huge amounts of memory, such as in the case of QKD based security systems.
The replacement system presented is stable in comparison with the high instability exhibited by the QKB based security systems.

References

[1]. A. Mink, S. Frankel, R. Perlner, "Quantum Key Distribution (QKD) and Commodity Security Protocols: Introduction and Integration"
[2]. D. Bouwmeester, A. Ekert, A. Zeilinger (Eds.), "The Physics of Quantum Information"
[3]. I. C. Boghitoiu, "Constructii electronica pentru amatori", Editura Albatros, 1989
[4]. Youtube video of the author presenting the hardware and its functioning related to the encryption system: https://www.youtube.com/watch?v=pK4kcCREgF4
[5]. C. H. Bennett and G. Brassard, in Proc. IEEE Int. Conf. Comp., "Systems and Signal Porcessing", 1984