Volume 2, Issue 3, March 2024 **ISSN (E):** 2938-3757

USING QUANTUM ALGORITHMS IN CRYPTOGRAPHY

Raupova M. H.
Tashkent Economic and Pedagogical Institute
Email: r.mokhinur@gmail.com

Abstract

The article addresses encryption algorithms based on the application of quantum particle physics rather than mathematical techniques, as well as the challenges that traditional cryptography approaches will encounter with the development of quantum computers. An overview of the most recent algorithms for quantum cryptography is given. The benefits and drawbacks of the suggested quantum algorithm-based information protection techniques are examined.

Keywords: quantum cryptography; uncertainty principle; post-quantum cryptography; photon.

Introduction

The first quantum key distribution technique, known as BB84, was created in 1984, marking the beginning of quantum cryptography as a scientific field. The primary benefit of quantum cryptography over classical cryptography protocols is a strict theoretical justification for their strength: whereas in classical cryptography the strength is typically based on assumptions about the computational capabilities of the interceptor, in quantum cryptography the interceptor can take any action permitted by natural laws and still not be able to obtain the secret key covertly.

An important property of quantum mechanics for quantum cryptography is the property of wave function collapse, which means that when any quantum mechanical system is measured, its initial state, generally speaking, changes. This leads to the important corollary that it is impossible to reliably distinguish quantum states from their non-orthogonal set. It is this property that is used to justify the secrecy of quantum cryptography: when trying to eavesdrop on transmitted states from their non-orthogonal set, the interceptor inevitably introduces an error into them, as a result of which it can be detected by additional interference on the receiving side. Therefore, the decision on the possibility of secret distribution of keys is achieved by legitimate users based on the magnitude of the observed error on the receiving side: as the value of this error approaches a critical value (depending on the protocol used), the length of the secret key in bits tends to zero, and key transfer becomes impossible.

This means that the most important characteristic of quantum cryptography protocols is the permissible critical error on the receiving side, up to which secret distribution of keys is possible: the larger it is, the more stable the quantum cryptography system is with respect to its own noise and eavesdropping attempts. An important result is finding the exact value of the critical error for the BB84 protocol, which turns out to be approximately 11%.

Today, classical cryptography more than reliably ensures the integrity and confidentiality of data. Due to the extremely widespread use of the RSA algorithm, one of the most important

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

offerings of cryptography is the difficulty of the problem of factoring large numbers. To date, no algorithm has been found that solves this problem quickly enough. Even the most powerful supercomputer would take thousands of years to factorize prime numbers or solve other mathematical problems on which they are based. But with the advent of a full-scale quantum computer, such problems can be solved in a few hours or even seconds. This is evidenced by the quantum factorization algorithm developed in 1994 by the American scientist Peter Shor. He proposed an algorithm that solves this problem with polynomial complexity on a quantum computer. The main reason for this phenomenal acceleration is the ability to use the so-called "quantum parallelism" to perform the fast Fourier transform, on which the most efficient known factorization algorithms are based. Finding this algorithm allows us to reduce the problem of factorization to the technological problem of building a quantum computer: if it can be built, the RSA encryption scheme will be unreliable. This puts the capabilities of public key encryption at great risk. It is worth noting, however, that no significant progress has been made in building a quantum computer over the past ten years.

The emergence of quantum computers will open up fundamentally new opportunities for humanity, but at the same time, existing methods of protecting information will lose their effectiveness. Despite the fact that quantum computers are just leaving the laboratory, the need to use quantum-safe, or, as it is also called, post-quantum cryptography, exists today. As will be clear from the following discussion, quantum key distribution protocols make it possible to generate completely secret keys between remote subscribers at an acceptable speed, which, for example, can violate the secrecy of the RSA algorithm.

The basic facts of quantum information theory, on which quantum cryptography is based, are interconnected statements about the impossibility of copying arbitrary quantum states and the impossibility of reliably distinguishing non-orthogonal states. In combination, these facts mean that attempts to distinguish quantum states from a non-orthogonal set lead to interference, which means that the actions of an interceptor can be detected by the magnitude of the error on the receiving side.

It is important to note that quantum cryptography does not make any assumptions about the nature of the eavesdropper's actions and the amount of resources available to him: it is assumed that the eavesdropper can have any resources and do all possible actions within the framework of the currently known laws of nature. This significantly distinguishes quantum cryptography from classical cryptography, which is based on limitations in the computing power of the eavesdropper. This chapter will review the BB84 quantum key distribution protocol and provide a scheme to prove its secrecy, and then discuss various classes of eavesdropper attacks. There are different approaches for quantum key distribution, but they can be divided into two main types, depending on the properties they use:

1. Preparation and measurement protocol

Measuring an unknown quantum state change, it in some way. This phenomenon is known as quantum indeterminism and underlies results such as the Heisenberg uncertainty principle and the no-cloning theorems. This can be used to calculate the amount of information that was intercepted and to detect whether a channel has been tapped.

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

2. Entanglement-Based Protocols

The quantum states of two or more separate objects can be combined in such a way that they are described by the combined quantum state rather than as an individual object. This is called entanglement and means that measurements on one object affect another. If a tangled pair of objects is shared between two participants, then intercepting any object changes the system as a whole, revealing the presence of third parties (and the amount of information they have obtained). [4]

The idea of using particle physics to protect information from theft and unauthorized access was first proposed in 1970 by Columbia University graduate student Stefan Weisner in his work “Conjugate coding.” 14 years later, Bennett and Brassard, based on Weisner’s work, published an article that described the BB84 quantum key distribution protocol. At the moment, many quantum cryptography algorithms have been developed; in this chapter, the quantum key distribution algorithms BB84 and B92 will be discussed and a scheme will be given to prove their secrecy.

The first quantum key distribution technique, known as BB84, was created in 1984, marking the beginning of quantum cryptography as a scientific field. The primary benefit of quantum cryptography over classical cryptography protocols is a strict theoretical justification for their strength: whereas in classical cryptography the strength is typically based on assumptions about the computational capabilities of the interceptor, in quantum cryptography the interceptor can take any action permitted by natural laws and still not be able to obtain the secret key covertly. This information can be intercepted without measuring or copying quantum particles because it is non-quantum.

BB84 is the first quantum key distribution protocol, which was developed in 1984. The information carriers are photons polarized at angles of 0.45,90,135 degrees. The protocol uses four quantum states of a two-level system to encode information, forming two conjugate bases:

$$+: |x\rangle = |0\rangle, \qquad |y\rangle = |1\rangle,$$

$$\times: |u\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |v\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

It is easy to check that these bases satisfy the unbiased condition, which informally reduces to the fact that from the point of view of one basis the states in the other are located symmetrically:

$$|\langle x|u\rangle|^2 = |\langle x|v\rangle|^2 = \frac{1}{2},$$

$$|\langle y|u\rangle|^2 = |\langle y|v\rangle|^2 = \frac{1}{2},$$

At this stage of state preparation, Alice randomly selects one of the specified bases, and then randomly selects a bit value: 0 or 1, and in accordance with this choice sends one of four signals:

- $|x\rangle$, if this basis is “+” and the bit value is 0
- $|y\rangle$, with the same basis and the bit value is 1
- $|u\rangle$, when the basis “×” and bit 0 are missing
- $|v\rangle$, if bit 1 is dropped in the “×” basis

As Alice sends each of these signals, she remembers her choice of basis and choice of bit, resulting in two random string bits on her side.

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

Bob, receiving each of the signals sent by Alice, makes one of two measurements on it at random, each of which can give a reliable result due to the orthogonality of the states inside each basis of Alice:

$$M_0^+ = |x\rangle\langle x|, \qquad M_1^+ = |y\rangle\langle y|,$$
$$M_0^\times = |u\rangle\langle u|, \qquad M_1^\times = |v\rangle\langle v|.$$

As a result, he has two lines: with which of the bases were chosen for measurement, and with the results of these measurements.

So, after transferring all states and taking measurements, Alice and Bob each have two rows. Here the coordination of bases occurs: through an open channel, Alice and Bob announce to each other their lines with the choice of bases, and they throw away the parcel in which their bases did not match. It should be noted that if the basis used to send the state by Alice coincided with the basis of Bob's measurement, then in the absence of interference in the communication channel, the results in their bit strings at the corresponding position will coincide, therefore, after the stage of matching the basis in the case of an ideal channel and the absence actions on the part of the interceptor, Alice and Bob must have the same bit strings.

If there were errors in the channel or an eavesdropper is trying to eavesdrop on information, Alice's and Bob's bitstrings may not match, so they must consistently reveal about half of their bitstrings to test. According to the central limit theorem, the error in the revealed bit sequence gives a fairly accurate estimate of the error in the entire sequence, and from it the probability of error in the remaining positions can be fairly accurately estimated. If the error value is greater than a certain value (protocol parameter), data transmission stops: this means that the interceptor has too much information about the key. Otherwise, Alice and Bob are faced with the task of obtaining a shared secret key. This task can be divided into two stages: first, error correction is performed, as a result of which Alice and Bob have matching bit strings. The second stage, called secrecy enhancement, aims to exclude information about the key that could get to the eavesdropper as a result of operations on the used quantum states or during error correction. This step should leave the eavesdropper with no information about Alice and Bob's shared bit string.

Let’s us be familiar with B92 algorithm. This algorithm by using polarized photons, the B92 QKD technique enables Alice and Bob to generate a secret shared key and detects Eve, the potential eavesdropper, who may have intercepted the quantum channel. Let us first present the basic information about the B92 algorithm, which uses two non-orthogonal states. Please note that in the BB84 algorithm, in the absence of interceptor actions and interference in the channel, the probability of an error on the receiving side before the bases are agreed upon is 25%. This is caused by the use of a “hard” configuration of two pairs of basis vectors. The purpose of the B92 algorithm is to be able to flexibly change this parameter depending on additional conditions, such as the length of the channel or its quality. This can in some cases help achieve higher data transfer speeds.

At each step of the B92 algorithm, Alice sends Bob one of two non-orthogonal states $|\psi_0\rangle$, $|\psi_1\rangle$, where $\langle\psi_0|\psi_1\rangle = \cos\eta$ – is the main parameter of the algorithm. Bob on his side performs a "three-outcome measurement":

$$M_0 = \frac{|\psi_1^{\perp}\rangle\langle\psi_1^{\perp}|}{1+\cos\eta} = \frac{I - |\psi_1\rangle\langle\psi_1|}{1+\cos\eta},$$
$$M_1 = \frac{|\psi_0^{\perp}\rangle\langle\psi_0^{\perp}|}{1+\cos\eta} = \frac{I - |\psi_0\rangle\langle\psi_0|}{1+\cos\eta},$$
$$M_? = I - M_0 - M_1.$$

When applying such a measurement over the indicated states, the first two outcomes will, in the absence of errors, correspond to the exact results, while the inconsistent outcome "?" does not provide useful information about the transmitted state. Parcels with such outcomes are discarded.

After transmitting all messages, Alice and Bob, just as happened in the BB84 protocol, consistently reveal part of their bit sequences and estimate the number of errors. If there are more than a certain threshold value, the execution of the protocol is interrupted, otherwise the completely secret key is extracted from the remaining part of the bit strings.

The most important property of the B92 protocol is the presence of a parameter - the angle η between signal states. The closer this angle is to $\pi/2$, the closer the protocol is to simple signal forwarding using orthogonal states. At the same time, the data transmission speed increases, but their resistance to interception decreases. When using small values of η, there is a high probability of obtaining inconsistent ones. outcomes, which reduces the data transmission speed, but significantly complicates the situation for the eavesdropper.

Summing up, we can confidently say that today classical cryptography algorithms have outstripped the capabilities of computer technology and fully cope with the tasks assigned to them in protecting information. But the advent of quantum computers will inevitably lead to changes in encryption methods. Otherwise, almost all existing systems will very soon be instantly hacked. At the same time, the emergence of quantum computing will affect the security of classical cryptographic algorithms in different ways: in public-key algorithms, protection will disappear completely, and in symmetric algorithms its effectiveness will decrease by at least half. Therefore, the need for the development of quantum and post-quantum algorithms is very high.

REFERENCES

1. Greenstein J.: The Quantum Challenge. - Dolgoprudny: Intelligence, 2008
2. Konoplev Yu. M., Sysoev S. S. Quantum computer simulator. http://qc-sim.appspot.com (access date: 11.03.2019).
3. Valiev K.A.: Quantum computers: hopes and reality. - M.; Izhevsk: Regular and chaotic dynamics, 2002
4. IBM Quantum Experience [Electronic resource] – URL: https://quantumcomputing.ibm.com/composer/new-experiment (access date 10.10.2020).
5. Sysoev S.S. Introduction to Quantum Computing. Quantum algorithms: textbook. Allowance. – St. Petersburg. : Publishing house St. Petersburg. University, 2019. – 144 p.
6. Garey M. R., Johnson D. S. 1979. Computers and Intractability: A Guide to the Theory of NP-Completeness. W. H. Freeman and Co.

7. Ozhigov Yu.I. Quantum computing: educational method. Allowance. – M.: Moscow State Publishing House. University, 2003. – 104 p.
8. Get started with IBM Quantum Experience [Electronic resource]. – URL: https://quantum-computing.ibm.com/docs (access date 10.10/2020).
9. Kaye F., Laflamme R., Mosca M. Introduction to quantum computing. – Moscow–Izhevsk: Regular and chaotic dynamics; Institute for Computer Research, 2009. – 360 p.
10. Preskill J. Lecture notes for "Physics 219/Computer Science 219. Quantum Computation" (Formerly Physics 229). http://www.theory. caltech.edu/people/preskill/ph229/index.html.
11. Kaiser S., Granad K. K15 Learning quantum computing in Python and Q# / trans. from English A. V. Logunova. – M.: DMK Press, 2021. – 430 p.
12. Farmonov, S.H., Bekmuratov, T., Muhamediyev, D. About the dodges plans of the continuous selective control // 2020 International Conference on Information Science and Communications Technologies, ICISCT 2020, 2020, 9351415.