Nikita Chekushkin
I. H. Olishevskiy, research supervisor
Dnipro University of Technology, Dnipro (Ukraine)

QUANTUM CRYPTOLOGY ISSUES

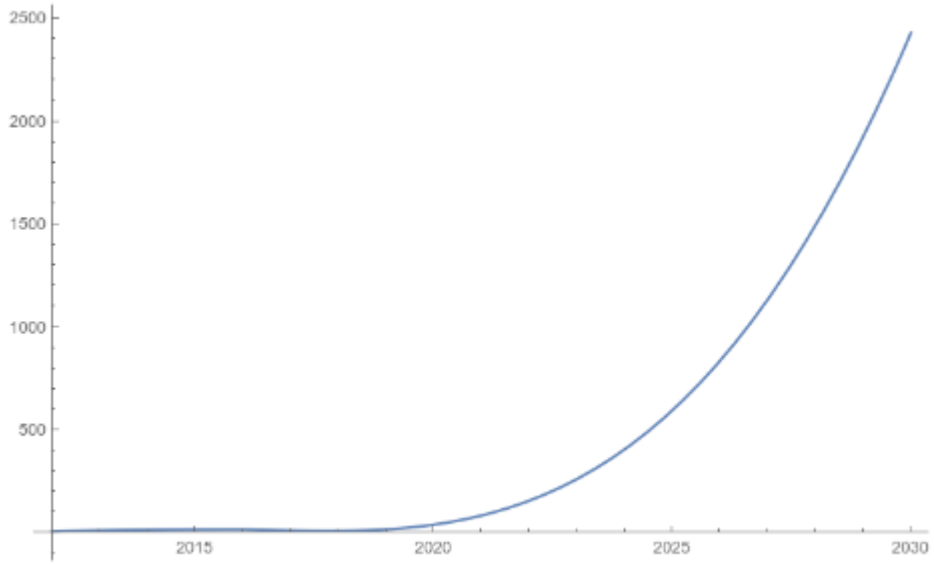
In the realities of the technological development of the digital environment, the role of data and information in them has changed significantly. Today, information is of tremendous importance both for international corporations and states, as well as for each of us, in particular. The issue of protecting information by transforming its appearance to prevent compromise (reading) by an outsider has been worrying the human race since ancient times. Cryptographic methods have become ubiquitous among all the ways to protect information from unauthorized persons. Cryptography is as old as human speech. Initially, writing itself was a cryptographic system, since in the ancient communes only a few owned it.

The answer to the question asked, where do the roots of cryptography come from and why this problem has become especially relevant in our time, lies in plain sight. We all use instant messengers and wish that the messages written by us remain only in dialogue with our interlocutor; so that when we pay for a purchase on the Internet using a bank card, its number remains only with us. And to ensure these security measures, asymmetric cryptography is used, which proved itself back in the middle of the last century with the "one-time pad" theory - which says that if the key is random, one-time and the number of key characters is equal to the number of characters of the text, then it is impossible to compromise such a message. The main idea of asymmetric cryptography lies in the fact that unilateral tasks are configured in it, they are easily solved in one direction and extremely difficult in the opposite direction. The most popular problem of this kind is the decomposition of a number into prime factors. Performing this action is more complicated than just multiplying two prime factors. This is laborious not only for the human mind but also for the central processor, moreover, if there are more than a hundred characters in the number.

In our world, there is such a thing that can still solve the inverse problem almost as quickly - a quantum computer. The most famous quantum computer algorithm is the Shor algorithm. The Shor algorithm was created to solve the problems of factorization of integers and discrete logarithms, that is, compared with a classical computer, the speed of solving inverse problems increases exponentially. If a quantum computer of sufficient power is created soon, the current encryption system will become unstable and, in a time slightly longer than that required for encryption, the Shor algorithm will crack cryptographic schemes such as (RSA, DSA, EdDSA, GOST R 34.10-2012 and others). Analyzing with the help of open data on the records of factorization of numbers, which are used as a public key in the RSA algorithm, it is clear that the quantum computer is gradually catching up with the standard one and, presumably, will surpass these indicators in 2030.

Year	Number(quantum pc)	Standard pc
2012	143(8 bit)	RSA - 768(768 bit)
2014	56135(16 bit)	-
2016	200099(18 bit)	-
2019	291311(18 bit)	RSA - 240(795 bit)
2020	1099551473989(41 bit)	RSA - 250(829 bit)

Pic. 1. Number factorization records



Pic. 2. Quantum computing on the factorization of RSA numbers

To solve this problem, two approaches exclude the human factor:

The first is post-quantum cryptography, which uses algorithms that will be resistant to the Shor algorithm. The disadvantages of this approach are that the proposed encryption method will be resistant only to the Shor algorithm, respectively, that another algorithm will be able to crack our developed

The second - Quantum Key Distribution is a security agreement of keys over an open communication channel, thanks to quantum mechanical systems. The use of quantum cryptography, or the so-called quantum key distribution. The principle of quantum encryption lies in a key distribution system that is mathematically proven to be impenetrable - even with all the unlimited computing power and technology, and they are limited only by the laws of physics. When there is a need to send a message with a length of 100 characters, you need to send 800 bits. To encrypt his computer takes single photons, encodes a bit into them, and sends them. Taking into account the loss of photons, they must be received and transmitted every 100 km, that is, trusted nodes should be arranged depending on the distance (every 100 km). An example of this is the quantum network between Shanghai and Beijing, which has 32 trusted nodes.

Key distribution speed and distance between transmitter and receiver are the key stumbling blocks of quantum cryptography today. Physicists are racking their brains over this dilemma, inventing more and more advanced protocols, new optical schemes, and methods for reading the quantum states of photons. It is also important to reduce the number of possible lost or incorrect photons. The critical mass is 11%. Due to the increasing distance between computers to which the quantum key is transmitted, more photons are damped. The necessary photons are lost and the rest of their mass remains, which is not related to the quantum key. Because of these highlights, it is impossible to transmit information over hundreds of kilometers in a real optical fiber.

Summing up, cryptography has gone far ahead from primitive ciphers to complex encryption algorithms, but this is not the limit of their development, since quantum computing is challenging and a new era of cryptography will come shortly. Given all the shortcomings, quantum cryptography can be used for distributed information storage. With its help, it becomes possible to distribute a certain amount of information across several clusters or servers and mix using quantum channels. If some of these clusters or data centers are compromised, the attacker will not receive complete information. Also, if some of the servers are disabled, the user who has access to manage these servers will be able to restore all the information. Quantum keys can also prove themselves in the protection of authentication,

when combining the blockchain technology of "hash functions" and quantum key distribution, they will allow you to check the user or the source of information, thereby protecting the system or account from penetration or compromise through a dummy user.

Sources

1. https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.98.010504
2. https://link.springer.com/article/10.1007/BF00191318
3. https://eclass.uoa.gr/modules/document/file.php/PHYS253/Bennett1992_Article_ExperimentalQuantumCryptograph.pdf
4. www.educba.com/algorithms-and-cryptography/