OVERVIEW OF THE CURRENT STATE OF QUANTUM INFORMATION SECURITY TECHNOLOGIES

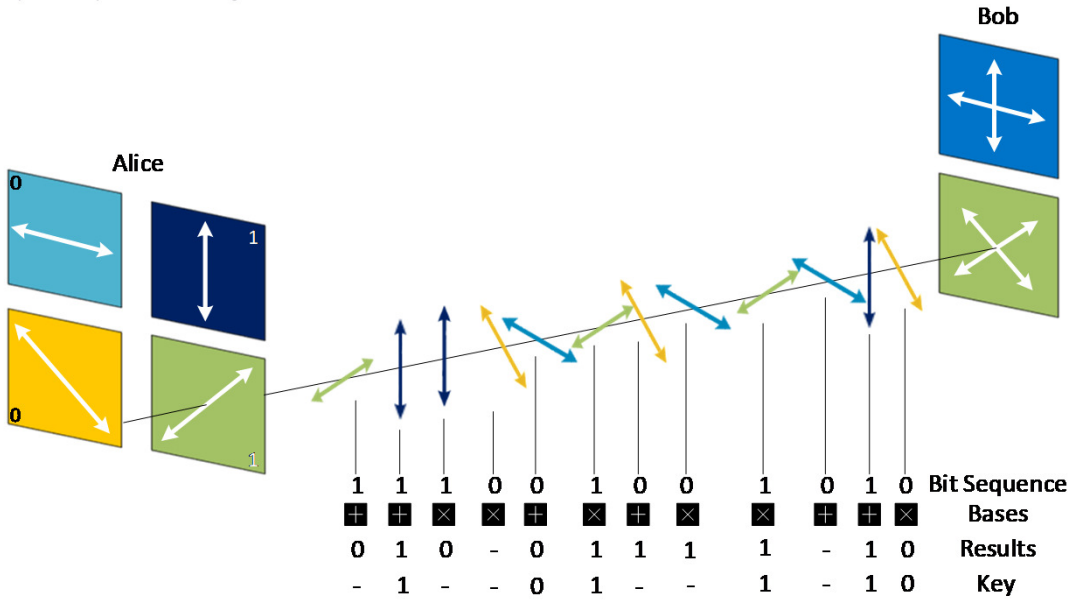
Dmytro Honchar[1], Yevhen Vasiliu[2]

[1] Postgraduate student, State University of Intelligent Technologies and Communications, Odessa, Ukraine, dmytro.honchar972@gmail.com
[2] Professor State University of Intelligent Technologies and Communications, Odessa, Ukraine, vasiliu@ua.fm

Considered the basic physical principles underlying quantum technologies of information security, the current state of their development and prospects for the implementation of new quantum crypto-primitives, as well as application of quantum key distribution technology in passive optical networks.

Introduction

Today, the issue of information security is especially relevant in view of the almost complete transition to digital technologies and the creation of the Internet of Things. The main encryption methods currently used are based on one very vulnerable assumption - all the security (secrecy) of these methods is based on the complexity of the computational algorithms used to decrypt the message, or in other words, the limited computing power of the attacker. This applies to both symmetric encryption and asymmetric encryption. The fundamental task in terms of encryption is the need to distribute keys. This is the main difference between encryption methods. The main principle in symmetric encryption systems is the condition that the transmitter and receiver know in advance the encryption algorithm, as well as the key to the message, without which the information is just a set of characters that do not make sense. This raises the issue of allocating encryption keys. There are two possible options for this: to encrypt the keys themselves, or to transmit the keys with the help of messengers (and hope that no one will intercept them on the way). Both key distribution options cannot be considered to fully meet future confidentiality requirements, but are widely used in engineering. In the case of a universal quantum computer, it is potentially possible to hack all modern cryptosystems. Currently, the transition to technologies based on the use of quantum effects is one of the main trends in modern communications and high performance computing. All over the world, great resources are being invested in the development of quantum methods of information transmission. This interest is due to the fact that even a partial transition to quantum technologies will make it possible to achieve fundamentally new qualities that are inaccessible when using classical approaches. Achievement of qualitatively new opportunities using the technology of quantum transmission and information processing is based on the laws of quantum physics that underlie them. Examples include "instantaneous" transmission of a quantum state at a distance based on the entanglement principle (quantum teleportation), acceleration of quantum computations due to their non-classical parallelism, and ensuring data confidentiality in quantum key distribution systems based on the indivisibility of quantum objects and the impossibility of their cloning.



At the moment, in classical cryptography there are no ciphers suitable for practical use that have unconditional security, and research on the creation of quantum computers is being carried out quite intensively, quantum cryptography is a rather promising field of cryptology. Today, devices for quantum key distribution are used in areas where a high level of security is required. Work is underway to create networks of trusted servers for quantum key distribution. Despite the unconditional strength of the theory of quantum key distribution, it has a number of disadvantages: the range and data transfer rate of quantum communication, the high cost of equipment. Of course, the quantum direction of cryptographic information protection is very promising, since quantum laws make it possible to bring information protection methods to a qualitatively new level. To date there is already experience in creating and testing a computer network protected by quantum-cryptographic methods - the only network in the world that is theoretically impossible to hack. Note that one of the longest quantum key distribution lines (more than 2000 km), containing 32 intermediate trusted servers, was built in China. As for other areas of quantum cryptography, including quantum secure feed forward and quantum secret sharing, they have not yet reached the level of practical use, despite this at the level of theoretical research, as well as at the level of laboratory experiments, all areas of quantum memory cryptography are rapidly developing and their practical implementation in the field of information security is likely to be a matter of one or two next decades.

Ministerstwo Edukacji i Nauki
Dofinansowano z programu „Doskonała nauka" Ministra Edukacji i Nauki