Example of quantum computer and security research paper

Sociology, Communication

Introduction

A quantum computer is a computing device, which work is based on the principles of quantum mechanics (Luca, n. d.). Traditional “ silicon” computers, with which, for example, is written, this paper, work on the basis of physical laws described in the arch of classical mechanics. Full-fledged quantum computers have not been yet created. So far only approaches to the creation of their architecture are developed.

The creation of quantum physics is considered one of the major scientific achievements of the XX century. Strictly speaking, the world uses quantum technologies for a long time and widely. These are lasers, complex LEDs, scanners and hypersensitive microscopes. But all of these devices are based on the “ mass” effect created by a huge group of elementary particles (or waves) that obey quantum laws. Using the effects observed for the individual particles (waves) will raise the technological progress to new heights. But the use of this potential is yet incredibly difficult task.

Quantum computers are not limited to binary coordinate system: calculation is made using qubits, which can be simultaneously in all its possible states (principles of quantum physics imply that one can only speak of the probability, not certainty, the existence of subatomic particles in some particular state in a given location). The calculation result is obtained by measuring the state of a quantum processor after the commission of a special type of operations (so-called “ unitary operations”) of qubits. Dozens of possible algorithms of work of such computer have already been described and specific programming languages are developed (Bonsor and Strickland, n. d.).

Security Issues

Computer security, security of information transfer, is the basis for the existence of the security of society. The information that people transfer via the network is often confidential. A quantum computer will solve not one, but many tasks, which are in a state of superposition. This makes it possible to achieve tremendous computing parallelism. If someone can build a computer based on quantum properties of matter, such a computer can run much faster than usual to solve a certain class of problems.

Quantum technologies provide not only a way to breach information networks, but also a way to support their safety. Quantum technology is not limited to the information sphere. Quantum technology in general is a technology that is based on the manipulation of complex quantum systems at the level of their individual components, and not just a technology based on quantum physics (Dunjko, Fitzsimons, Portmann and Renner, 2014). Assume the transistor, according to this definition, is not a quantum technology because, although it is based on quantum physics, there is no control of individual electrons, and quantum technologies are spoken about managed quantum particles.

Currently, cryptography can be considered one of the extremely vital issues in the majority of protected electronic communication systems, as it guarantees that only genuine parties can read each other’s switched messages. Quantum computing warns the essential objective of protection, genuine communication since in being capable of do definite kinds of calculations that traditional computers are not able. Quantum computer can rapidly damage cryptographic keys, so this permits an eavesdropper to pay

attention to confidential communications and imagine being an important person whom he is not. It is worth to mention that quantum computers achieve this by rapidly overturn calculating or supposing secret cryptographic keys, an assignment that is measured very tough and unlikely for a traditional computer (Quantum Safe Cryptography and Security).

A quantum computer perhaps could be stand on the table of every hacker very long ago, but the creation of a computer associated with a number of purely engineering difficulties is so great that some experts believe the creation of " high-grade" quantum computer is impossible task. The main problem is to maintain the qubits in a state of confusion, as any quantum system continually strives to " fall" into the classical devoid of uncertainty. Here suffering Schrödinger's cat should be mentioned, which still cannot be alive and dead at the same time, and in a quantum computer this wonderful state should be maintained long enough to run the tasks and measure the results. Typically, it is about nanoseconds, in the best systems – units of seconds. The complexity of the problem increases with the number of qubits. To meet the challenges of breaking ciphers a quantum computer with 500-2000 qubits is required (depending on bit key in the cryptographic algorithm), while most of the existing systems operate with units of qubits (record – 14 qubits). Thus, hacking SSL-certificate on a quantum computer today is still impossible, but it may be real in a couple of years.

Thus, many people believe that a quantum computer is the same as traditional computer, but only faster. This is absolutely not the case, since a quantum computer is mainly not an instrument of creation, but destruction weapon, the atomic bomb of the information age. However, it is actually very

hard to develop. This is perhaps the most distant and most complex of the existing quantum technologies. In fact, quantum technologies offer the world a way of not only the destruction of the information structure of society, but also a way to protect against hacking. There is such a technology, such as quantum cryptography, the idea of which is that the information is transmitted by means of elementary particles of light – photons. In other words, each bit is carried by one photon somehow. And if there is a hacker who tries to steal or measure the condition of those photons, and accordingly, know the transmitted message, the hacker will inevitably destroy these photons, because the hacker is large and photons are small. And so he is bound to be seen, and a violation of information security can be prevented (Quantum Safe Cryptography and Security).

Conclusion

A quantum computer is not just a computer of the future generation, it is much more not only in terms of the use of the latest technology, but also in terms of its unlimited, incredible, fantastic features that cannot only change the world of people, but even create a different reality. For practical application any quantum computer has not been created yet. However, in many developed countries, the development of quantum computers is paid close attention and such programs are annually invested by tens of millions of dollars (Aaronson, 2008).

Thus, modern Internet ensures the privacy by using cryptographic keys. A fairly large part is based on public key technologies. This technology is based on the fact that to decrypt the key of certain length is difficult with modern

computer technology, but if these technologies improve, people will be able to decipher the key, and then the bank transfers will be unsafe. Quantum communication lines offer another principle: they offer to send information encoded in single particles, photons. Quantum mechanics prohibits copying quantum-mechanical particles. They can be measured only once. If someone tries to measure and send the same one, then it can be done only with an error that will be immediately noticeable.

References

Aaronson, S. (2008). The Limits of Quantum. Retrieved from http://www. cs. virginia. edu/~robins/The_Limits_of_Quantum_Computers. pdf

Bonsor, K. and Strickland, J. (n. d.). How Quantum Computers Work. Retrieved from http://computer. howstuffworks. com/quantum-computer. htm

Dunjko, V., Fitzsimons, J. F., Portmann, Ch. and Renner, R. (2014). Composable security of delegated quantum computation. Retrieved from http://arxiv. org/pdf/1301. 3662. pdf

Luca, M. (n. d.). Quantum Computers: A Brief Overview. Retrieved from http://www. student. montefiore. ulg. ac. be/~merciadri/docs/papers/quantum-computers. pdf

Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges. Retrieved from http://docbox. etsi. org/Workshop/2014/201410_CRYPTO/Quantum_Safe_Whitepaper_1_0_0. pdf